UNITED
NATIONS

A

General Assembly

Distr.
GENERAL

A/CN.9/446
11 February 1998

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Thirty-first session
New York, 1-12 June 1998

REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-SECOND SESSION (Vienna, 19-30 January 1998)

CONTENTS

	Paragraphs	Page
INTRODUCTION	1-11	3
I. DELIBERATIONS AND DECISIONS	12-13	5
II. INCORPORATION BY REFERENCE	14-24	6
III. CONSIDERATION OF DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES	25-207	10
CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS	25-26	10
CHAPTER II. ELECTRONIC SIGNATURES	27-106	10
Section I. Secure electronic signatures	27-61	10
Article 1. Definitions	27-46	10
Article 2. Presumptions	47-48	16
Article 3. Attribution	49-61	17

V.98-50891

	Paragraphs	Page
Section II. Digital signatures	62-86	21
Article 4. Definition	62-70	21
Article 5. Effects	71-84	23
Article 6. Signature by legal persons	85-86	28
Section III. Other electronic signatures	87-106	28
CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES	107-174	33
Article 7. Certification authority	107-112	33
Article 8 Certificate	113-131	35
Article 9. Certification practice statement	132-133	39
Article 10. Representations upon issuance of certificate	134-145	40
Article 11. Contractual liability	146-154	45
Article 12. Liability of the certification authority to parties relying on certificate	155-173	47
Articles 13 to 16	174	53
CHAPTER IV. RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES	175-207	53
Article 17. Foreign certification authorities offering services under these Rules	175-188	53
Article 18. Endorsement of foreign certificates by domestic certification authorities	189-195	56
Article 19. Recognition of foreign certificates	196-207	58
IV. COORDINATION OF WORK	208-211	61
V. FUTURE WORK	212-213	62

INTRODUCTION

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that work to be carried out by the Working Group at its thirty-first session (New York, 18-28 February 1997) could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the scope of the uniform rules to be prepared. As to a more precise mandate for the Working Group, it was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [1/]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). As to the desirability and feasibility of preparing uniform rules on issues of digital signatures and certification authorities, the Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While it had not made a firm decision as to the form and content of such work, it had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (see A/CN.9/437, paras. 156-157). With respect to the issue of incorporation by reference, the Working Group concluded that no further study by the Secretariat was needed, since the fundamental issues were well known and it was clear that many aspects of battle-of-forms and adhesion contracts would need to be left to applicable national laws for reasons involving, for example, consumer protection and other public-policy considerations. The Working Group was of the opinion that the issue should be dealt with as the first substantive item on its agenda, at the beginning of its next session (A/CN.9/437, para. 155).

3. The Commission expressed its appreciation for the work already accomplished by the Working Group at its thirty-first session, endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities (hereinafter referred to as "the Uniform Rules").

4. With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken

in the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"). Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought.

5. As an additional item to be considered in the context of future work in the area of electronic commerce, it was suggested that the Working Group might need to discuss, at a later stage, the issues of jurisdiction, applicable law and dispute settlement on the Internet. [2/]

6. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-second session at Vienna from 19 to 30 January 1998. The session was attended by representatives of the following States members of the Working Group: Algeria, Australia, Austria, Brazil, Bulgaria, China, Egypt, Finland, France, Germany, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Mexico, Nigeria, Poland, Russian Federation, Singapore, Slovakia, Spain, Sudan, Thailand, United Kingdom of Great Britain and Northern Ireland and United States of America.

7. The session was attended by observers from the following States: Angola, Belarus, Bosnia and Herzegovina, Canada, Colombia, Costa Rica, Czech Republic, Denmark, Greece, Guatemala, Indonesia, Iraq, Ireland, Kuwait, Lebanon, Malaysia, Morocco, Netherlands, Pakistan, Paraguay, Republic of Korea, Sweden, Switzerland, Turkey and Ukraine.

8. The session was attended by observers from the following international organizations: International Trade Centre UNCTAD/WTO, United Nations Conference on Trade and Development (UNCTAD), United Nations Educational, Scientific and Cultural Organization (UNESCO), United Nations Industrial Development Organization (UNIDO), World Intellectual Property Organization (WIPO), European Commission, Organisation for Economic Co-operation and Development (OECD), World Trade Organization (WTO), Cairo Regional Centre for International Commercial Arbitration, *Comité Maritime International* (CMI), International Association of Ports and Harbors (IAPH), International Bar Association (IBA), International Chamber of Commerce (ICC), Internet Law and Policy Forum (ILPF) and European Law Student Association (ELSA) International.

9. The Working Group elected the following officers:

Chairman: Mr. Mads Bryde ANDERSEN (Denmark);

Vice-Chairman: Mr. PANG Khang Chau (Singapore);

Rapporteur: Mr. Gritsana CHANGGOM (Thailand).

10. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.72); a note prepared by the Secretariat for the thirty-first session of the Working Group under the title "Planning of future work on electronic commerce: digital signatures, certification authorities and related legal issues" (A/CN.9/WG.IV/WP.71), which summarized previous deliberations by the Working Group on the issue of incorporation by reference; a note reproducing the text of a proposed draft provision on incorporation by reference and explanatory comments by the United Kingdom of Great Britain and Northern Ireland (A/CN.9/WG.IV/WP.74); and a note by the Secretariat containing draft uniform rules on digital signatures, other electronic signatures, certification authorities and related legal issues (A/CN.9/WG.IV/WP.73).

11. The Working Group adopted the following agenda:

1. Election of officers

2. Adoption of the agenda

3. Legal aspects of electronic commerce:
incorporation by reference

4. Legal aspects of electronic commerce:
draft uniform rules on digital signatures,
other electronic signatures, certification authorities
and related legal issues

5. Other business

6. Adoption of the report.

I. DELIBERATIONS AND DECISIONS

12. The Working Group discussed the issue of incorporation by reference on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP.71) and the proposal made by the United Kingdom of Great Britain and Northern Ireland (A/CN.9/WG.IV/WP.74). The deliberations and conclusions of the Working Group with respect to that issue are reflected in section II below. After discussion, the text of a draft article on incorporation by reference was adopted by the Working Group. The Secretariat was requested to prepare, on the basis of the deliberations and decisions of the Working Group, a short guide to assist States in enacting and applying the draft article. It was noted that the draft article, together with the relevant guide to enactment, would be placed before the Commission at its thirty-first session, to be held in New York from 1 to 12 June 1998, for final review and possible insertion in the Model Law and its Guide to Enactment.

13. The Working Group also discussed the issues of digital signatures, other electronic signatures, certification authorities and related legal issues on the basis of the note prepared by the

Secretariat (A/CN.9/WG.IV/WP. 73). The deliberations and conclusions of the Working Group with respect to those issues are reflected in section III below. The Secretariat was requested to prepare, on the basis of those deliberations and conclusions, a set of revised provisions, with possible variants, for consideration by the Working Group at a future session.

II. INCORPORATION BY REFERENCE

14. Having recalled its earlier deliberation of the matter of incorporation by reference, and the draft texts proposed as its previous sessions (A/CN.9/WG.IV/WP.71, paras. 77-93), the Working Group was invited to consider the matter of incorporation by reference in an electronic context on the basis of a proposed draft provision (A/CN.9/WG.IV/WP.74, Annex), which read as follows:

"(1) This article applies when a data message contains reference to, or its meaning is only fully ascertainable by reference to, information recorded elsewhere ('the further information').

"(2) Subject to paragraph (5), the data message shall have the same effect as if the further information were fully expressed in the data message and any reference to the data message will constitute a reference to that message including all further information, if the conditions in paragraph (3) are satisfied.

"(3) The conditions mentioned in paragraph (2) are that the data message:

"(a) identifies the further information -

"(i) by a collective name or description or code; and

"(ii) by specifying adequately the record, and the parts of that record, containing the further information and, where that record is not publicly available, the place where, and, in cases where the means of access is either not obvious or is restricted in some way, the means by which, it may be found; and

"(b) expressly indicates or carries a clear implication that the data message is intended to have the same effect as if the further information were fully expressed in the data message.

"(4) The identification mentioned in paragraph (3)(a) may be made indirectly, by referring to information recorded elsewhere which contains the necessary identification, provided the conditions in paragraph (3) are satisfied with respect to that reference.

"(5) Nothing in this article affects -

"(a) any rule of law which requires adequate notice to be given of the content of the further information, or of the record or place where, or the means by which such information may be found, or which requires that place or record to be accessible to another person; or

"(b) any rule of law relating to the validity of terms for the purpose of contract formation, including the acceptance of an offer.

"(c) any rule of law prescribing the effectiveness of the further information being incorporated or the validity of the process of incorporation."

15. It was observed that: the draft provision was intended to apply when a data message used incorporation by reference (para. (1)); the overall principle was that the incorporated information (not referred to as "terms or conditions", since not all information created an obligation) should have the same effect as if it were fully expressed in a data message (para. (2)); the general conditions for incorporation by reference should be clear and precise identification of the information being incorporated (which was of particular importance for the protection of consumers and other third parties), identification of where and how that information could be accessed and an indication of intent to incorporate (para. (3)); indirect identification of the source of information by reference to another source should be acceptable under the same conditions (para. (4)); and that any existing rules of law applying to incorporation by reference in paper communications should extend to electronic communications (para. (5)).

16. It was generally agreed that the matter had to be dealt with, since incorporation by reference was inherent in the use of electronic communications. It was stated that in electronic communications large amounts of data were by necessity incorporated by reference (e.g., communication records, policy statements, digital signatures in certificates). In addition, it was observed that incorporation by reference in an electronic context could be satisfied by various methods, including, but not limited to, uniform resource locators (URLs), object identifiers (OIDs) or other records reasonably available at a stated address.

17. While it was admitted that incorporation by reference created certain risks, e.g., for consumers, it was argued that, at the same time, such practice allowed consumers to take advantage of opportunities offered only via electronic communication networks. The main goal of a provision on incorporation by reference, it was pointed out, should be to establish a balance among the interested parties. With a view to achieving that goal, the Working Group was invited to consider, in parallel with the above-mentioned draft provision, a draft provision along the following lines:

"Variant A Unless otherwise agreed between the parties, information is regarded as forming part of a data message, if expressly indicated or clearly implied [and if that data message indicates a procedure whereby that information can be accessed in a reasonable and timely manner]. Such information is effective to the extent permitted by law.

"Variant B Information shall not be denied legal effect solely on the grounds that it is incorporated by reference in a data message."

18. With regard to Variant A, it was stated that the material factors bearing on whether a term was reasonably accessible included: availability (hours of operation of the repository, ease of access, and acceptable levels of redundancy); cost of access (excluding underlying communications service costs; if there was a cost it should be reasonable and in proportion with the value associated with the contract); format (widely used within the community of interest); integrity (verification of content, authentication of sender, and mechanism for communication error correction); and the extent to which it was subject to later amendment (without a contractual right to do so; notice of updates; notice of policy of amendment). Those factors, it was added, could be set forth in a guide to enactment of the provisions on incorporation by reference (see below, paras. 23-24).

19. The Working Group proceeded with its discussion on the basis of the above-mentioned proposals for alternative provisions. It was observed that the proposed draft provisions had a number of advantages in common. One such advantage was that they were intended to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference were applicable to incorporation by reference in an electronic environment. In that connection, it was suggested that a different approach might be taken, to the effect that wide use of incorporation by reference would be discouraged in an electronic environment, thus reducing the risk that the difficult situation known as "battle of forms" in traditional paper-based trade might be replicated in electronic commerce. In support of that suggestion, it was observed that, while in a paper-based context incorporation by reference was necessary for time, space and cost reasons, in an electronic context a large amount of data could be reflected in data messages in a simple, timely and inexpensive manner. That suggestion was objected to on the grounds that it would be inappropriate for a uniform law to play the role of a code of conduct, thus discouraging the use of a widespread and important practice, the use of which was inherent in electronic communications.

20. Another advantage of the above-mentioned proposals, it was said, was that they recognized that consumer-protection or other national or international law of a mandatory nature (e.g., rules protecting weaker parties in the context of contracts of adhesion) should not be interfered with. It was pointed out that: the first proposal was intended to achieve that result by listing rules of law that remained unaffected (para. (5)); and that the second proposal led to the same result, since it referred to information being effective "to the extent permitted by law" (Variant A), or did not preclude that information be denied legal effect on grounds other than incorporation by reference (Variant B). With a view to making it overly clear that existing law was not affected by any of the proposed wordings, it was suggested that any provision on incorporation by reference should be subjected to language along the lines of the second footnote to article 1 of the Model Law, which stated expressly the principle that the Model Law was not intended to override consumer-protection law.

21. However, the view was expressed that the first proposal and Variant A of the second proposal presented a number of disadvantages. One disadvantage was that they ran the risk of upsetting well-established or emerging practices by setting too high a standard. It was stated that in

many practices it would be impossible to meet the requirements for an express indication or a clear implication of intention that the information be incorporated by reference or for reasonable accessibility to that information. The example was mentioned of the incorporation by reference of a main charter-party in a bill of lading delivered under a sub-charter-party, a practice that was said would be hampered by requirements for an express indication or a clear implication of intention that the information be incorporated by reference or for reasonable accessibility to that information. Another disadvantage was that those provisions might inadvertently interfere with mandatory rules of law and lead to unfair results. In that connection, it was pointed out that, in addition to the two conditions set forth in the first proposal and in Variant A of the second proposal, a third element should be included, namely that incorporation by reference should be subject to acceptance by the parties. In particular in open EDI, it was stated, acceptance by the parties was essential.

22. In response, it was observed that paragraph (5) of the first proposal and the second sentence of Variant A of the second proposal were intended to address exactly those concerns and to ensure that the provision on incorporation by reference would not interfere with established practices or with mandatory rules of national law. However, it was felt that those provisions might raise questions of interpretation. Variant B, it was observed, did not present that disadvantage, in that it merely expressed the general principle of non-discrimination enshrined in article 5 of the Model Law. It was generally recognized that Variant B implied that incorporation by reference would be effective only to the extent permitted by law. On that basis, the Working Group generally agreed that Variant B would be preferable.

23. As a matter of drafting, it was suggested that Variant B should parallel the language of article 5 of the Model Law and thus refer, not only to legal effect, but also to validity and enforceability. With regard to the location of the provision on incorporation by reference, it was suggested that, in view of the fact that the issue related to electronic commerce in general and not only to digital signatures, it should be inserted in the Model Law as a new article 5 bis. In order to assist users of the Model Law and legislators in the interpretation of the provision on incorporation by reference, it was also suggested that the background and explanatory information with regard to the provision on incorporation by reference should be included in the Guide to Enactment of the Model Law. The suggestion was made that the guide could indicate the factors on the basis of which States might wish to adopt an expanded version of the provision on incorporation by reference. Such factors could be inspired from the text of the first proposal and Variant A of the second proposal. That suggestion was found to be generally acceptable. However, a note of caution was struck that such an approach might be inconsistent with the approach taken in article 5 of the Model Law. The view was expressed that the above-mentioned factors should not be set out as alternatives to the provisions of the Model Law. It was generally felt that, in drafting the portion of the Guide to Enactment dealing with incorporation by reference, attention should be given to avoiding inadvertently suggesting that restrictions to incorporation by reference should be introduced with respect to electronic commerce in addition to those that might already apply in paper-based trade.

24. After discussion, the Working Group adopted Variant B, decided that it should be presented to the Commission for review and possible insertion as a new article 5 bis of the Model Law and requested the Secretariat to prepare a explanatory note to be added to the Guide to Enactment of the Model Law.

III. CONSIDERATION OF DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS

25. The Working Group generally agreed that the relationship between the Uniform Rules and the Model Law (in particular, the question whether the Uniform Rules on digital signatures should constitute a separate legal instrument or whether they should be incorporated in an extended version of the Model Law) would need to be clarified at a later stage. While it was agreed that no decision could be made at this stage, the Working Group confirmed its working assumption that the Uniform Rules should: be prepared as draft legislative provisions; be consistent with the provisions of the Model Law in general; and somehow incorporate provisions along the lines of articles 1 (Sphere of application), 2(a),(c) and (e) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation) and 7 (Signature) of the Model Law.

26. With respect to the sphere of application of the Uniform Rules, the view was expressed that it should be limited to digital signatures, to the exclusion of other authentication techniques. It was recalled in response that, in making its preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules on digital signatures, the Working Group, at its previous session, had also agreed that, alongside digital signatures and certification authorities, work in the area of electronic commerce might need to address issues of technical alternatives to public-key cryptography (see A/CN.9/437, paras. 156-157). It was also recalled that, at the thirtieth session of the Commission, it was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken in the Model Law (see above, para. 4). After discussion, the Working Group confirmed its decision that, while focusing on the preparation of specific provisions dealing with digital signature techniques, it should also extract from those specific provisions rules of more general application to accommodate alternative authentication techniques.

CHAPTER II. ELECTRONIC SIGNATURES

Section I. Secure electronic signatures

Article 1. Definitions

27. The text of draft article 1 as considered by the Working Group was as follows:

"For the purposes of these Rules:

"(a) 'Signature' means any symbol used, or any security procedure adopted by

[or on behalf of] a person with the intent to identify that person and to indicate that person's approval of the information to which the signature is appended;

"(b) 'Electronic signature' means [a signature][data] in electronic form in, or attached to, or logically associated with, a data message [and used by [or on behalf of] a person with the intent to identify that person and to indicate that person's approval of the contents of the data message][and used to satisfy the conditions in [article 7 of the UNCITRAL Model Law on Electronic Commerce]];

"(c) 'Secure electronic signature' means an electronic signature which

"(i) is a digital signature under article 4 and meets the requirements set forth in article 5; or

"(ii) as of the time it was made, can otherwise be verified to be the signature of a specific person through the application of a security procedure that is: uniquely linked to the person using it; capable of promptly, objectively and automatically identifying that person; created in a manner or using a means under the sole control of the person using it; and linked to the data message to which it relates in a manner such that if the message is altered the electronic signature is invalidated; or

"(iii) [as between parties involved in generating, sending, receiving, storing or otherwise processing data messages in the ordinary course of their business,] is commercially reasonable under the circumstances, previously agreed to, and properly applied, by the parties."

General remark

28. It was pointed out that the provisions contained in draft article 1 were intended not only as definitions but also as a means of delineating the scope of the Uniform Rules. While it was noted that the same drafting technique had been used in the context of the Model Law, it was generally felt that draft article 1 might need to be revisited by the Working Group during its deliberation of the scope of the Uniform Rules.

Subparagraph (a)

29. It was widely felt that subparagraph (a) should be deleted. While including in the Uniform Rules a definition of "signature" based on article 7 of the Model Law might provide useful guidance in those countries where there currently existed no definition of a "signature", it was stated that such a definition was not necessary for the purposes of the Uniform Rules. One of the reasons stated for deletion was that including an all-purpose definition of "signature" might jeopardize the acceptability of the instrument in those countries where the provision contained in subparagraph (a) might conflict with existing definitions.

Subparagraph (b)

30. It was widely felt that the wording of subparagraph (b) should mirror the text of article 7 of the Model Law. That result could be achieved either by reproducing that article in full in subparagraph (b) or by way of a reference to "the conditions set forth in article 7 of the Model Law". After discussion, the Working Group found the latter formulation to be preferable. As a matter of drafting, it was generally agreed that the word "data" should be used instead of the words "a signature".

Subparagraph (c): general remarks

31. The view was expressed that defining an electronic signature as "secure" might be inappropriate. Whether a given technique was "secure" was not a matter of definition but a question of fact to be determined in relation to the circumstances under which that technique was used. The use of the word "secure" was also criticised on the grounds that it introduced a subjective criterion and that it implied that signatures that did not fall within that category were inherently insecure. In response, it was stated that, while the reference to a "secure" signature might need to be replaced by better wording, it was only used in the Uniform Rules as a means of delimiting a category of electronic signatures of a quality such that specific legal effects could be attached to them. As to whether the use of the word "secure" might establish a subjective criterion, it was stated that authentication techniques did not develop in a vacuum. Standards implemented either through regulation or through voluntary, industry-based practices would be available to assess the degree of security of any given technique. After discussion, the Working Group decided to proceed on the assumption that a category (provisionally labelled "secure") would be used to address the range of techniques to which the Uniform Rules would attach certain legal effects.

32. The view was expressed that it might be inappropriate to provide that the same legal effect would attach to the use of a wide variety of authentication techniques, which were said to range from inherently secure (e.g., digital signatures) to inherently insecure (e.g., certain authentication techniques that might be agreed upon by the parties). In response, it was stated that subparagraph (c) was precisely aimed at creating a category where the most secure among digital signatures could be placed on an equal footing with other techniques, provided that those techniques met the severe standard set forth in subparagraph (c)(ii). As to subparagraph (c)(iii), consideration might be given to placing it in a separate provision dealing with party autonomy. It was agreed that the discussion on the definitions might need to be reopened after the provisions dealing with the legal effects of those definitions had been considered.

Subparagraph (c)(i)

33. The substance of subparagraph (c)(i) was found to be generally acceptable. However, the view was expressed that the requirements of draft article 5 referred to in subparagraph (c)(i) did not adequately ensure the quality of digital signatures as secure electronic signatures. It was suggested that the question would have to be revisited in the context of draft article 5.

Subparagraph (c)(ii)

34. A concern was expressed that the burden of proof under subparagraph (c)(ii) was so high that the presumptions in draft article 2(1) would be of little meaning in the case where non-digital electronic signatures were used. It was stated in response that subparagraph (c)(ii) and draft article 2 were intended to serve different purposes. It was generally agreed, however, that the relationship between subparagraph (c)(ii) and draft article 2 might need to be clarified in the revised draft of the Uniform Rules to be prepared by the Secretariat.

35. It was generally felt that the substance of subparagraph (c)(ii) was important to guarantee the media-neutrality of the Uniform Rules. The view was expressed that, since the purpose of subparagraph (c)(ii) was to define certain criteria which a given technique should meet to trigger the presumptions set forth in draft article 2, it was irrelevant whether that technique was used with an intent to sign. Accordingly, it was suggested that the words "can otherwise be verified to be the signature of a specific person" should be deleted.

36. Additional suggestions were made as to the specific formulation of subparagraph (c)(ii). One suggestion was that the words "promptly" and "automatically" should be deleted. It was stated that "prompt" and "automatic" identification of a person were not inherent in the use of most authentication techniques (including certain digital signature techniques) and did not clearly relate to the security of the authentication procedure and the integrity of the data being electronically signed. Another suggestion was that the words "of a security procedure" should be complemented by the words "or combination of security procedures". After discussion, those suggestions were adopted by the Working Group.

Subparagraph (b)(iii)

37. It was suggested that subparagraph (iii) should be deleted. It was stated that granting the status of a "secure electronic signature" to any procedure which might be agreed upon by the parties would create the risk that any low-security procedure could be used to produce legal effects. In that connection, the view was expressed that, currently, the only "secure" authentication technique was that of a digital signature. In response, it was observed that, as a matter of freedom of contract, parties should be free to agree that, as between themselves, they would rely on an authentication technique that was less secure than the type of electronic signature described in subparagraph (c)(ii), and that they would attach the presumptions set forth in draft article 2 to the use of that authentication technique. It was also observed that the reference to the "commercial reasonableness" of the signature technique was intended to provide a safeguard against the unlimited recognition of possibly insecure authentication techniques through party autonomy. A note of caution was struck, however, about relying on the notion of "commercial reasonableness" to provide such a safeguard. In a number of countries, the mere fact that "commercial" parties had agreed on a procedure would be sufficient to interpret that procedure as "commercially reasonable". As a matter of drafting, a question was raised as to a possible inconsistency between the use of the words "commercially reasonable" and the wording used in article 7 of the Model Law. While it was recalled that the words "commercially reasonable" had been used in article 5 of the UNCITRAL Model Law on International Credit Transfers, the Working Group felt that appropriate

redrafting might be needed to avoid the above-mentioned interpretation. It was suggested that a reference to an express stipulation by the parties that the agreed technique would have the effects of a secure electronic signature under draft article 2 might need to be included in subparagraph (c)(iii). It was also suggested that the words "as between parties" should be maintained in subparagraph (c)(iii) without square brackets.

38. A question was raised as to whether subparagraph (c)(iii) might be used by the parties to deviate from mandatory rules of law regarding the form of certain legal acts. It was stated that such an interpretation would be unacceptable in view of the fact that such freedom of contract did not exist in a paper-based environment. While it was generally agreed that, under the law of a number of countries, certain mandatory form requirements could not be deviated from by private agreement, such mandatory form requirements typically applied to a very narrow category of transactions, which could probably be dealt with by way of express exclusion from the scope of a general provision dealing with party autonomy.

39. The discussion focused on the manner in which party autonomy would be dealt with in the Uniform Rules. It was recalled that the mere reference to article 4 (Variation by agreement) of the Model Law might not suffice to provide a satisfactory solution, in view of the fact that article 4 established a distinction between those provisions of the Model Law that might be freely varied by contract and those provisions that should be regarded as mandatory unless variation by agreement was authorized by the law applicable outside the Model Law. With respect to electronic signatures, the practical importance of "closed" networks made it necessary to provide wide recognition of party autonomy. However, public policy restrictions on freedom of contract, including laws protecting consumers from overreaching contracts of adhesion, might also need to be taken into consideration. A suggestion was made that the Uniform Rules should include a provision along the lines of article 4(1) of the Model Law to the effect that, except as otherwise provided by the Uniform Rules or other applicable law, electronic signatures and certificates issued, received or relied upon in accordance with procedures agreed among the parties to a transaction would be given the effect specified in the agreement. In addition, it was suggested that the Working Group might consider establishing a rule of interpretation to the effect that, in determining whether a certificate, an electronic signature or a data message verified with reference to a certificate, was sufficiently reliable for a particular purpose, all relevant agreements involving the parties, any course of conduct among them, and any relevant trade usage should be taken into account.

40. As an alternative, the Working Group was invited to consider a proposed new article that read along the following lines:

> "(1) Where the law requires the signature of a person, that requirement is met by an electronic signature if
>
> > "(a) use of the electronic signature was agreed among the parties to the transaction, or
> >
> > "(b) the electronic signature was as reliable as was appropriate for the purpose for which the electronic signature was used.

"(2) In determining whether an electronic signature is appropriately reliable for a particular purpose, any course of conduct among the parties and any relevant trade usage shall be taken into account."

41. The discussion continued on the basis of the proposed new article. It was stated that the proposed text was intended to build on, and expand, the approach followed in article 7 of the Model Law. In particular it was stated that: paragraph (1)(a) was intended to enable parties to determine the type of electronic signature they wished to use in their business transactions; paragraph (1)(a) was inspired by article 7(1)(b) of the Model Law; and paragraph (2) constituted an effort to explain paragraph (1)(b). The view was expressed that, if the proposed new article were to be included in the Uniform Rules, paragraph (2) of draft article 2 of the Uniform Rules would not be necessary and could be deleted.

42. The proposal was generally objected to on the grounds that it clearly ran counter to article 7 of the Model Law in several ways, including that: it failed to include the elements of identification and approval, thus calling signature something that, in the light of the Model Law, was not a signature; it allowed parties to derogate from mandatory rules of law relating to signatures, thus overriding rules that, under article 7(2) of the Model Law, could establish an obligation for, or legal consequences in the absence of, a signature; and it failed to include a provision along the lines of article 7(3) of the Model Law, which allowed States to exclude the application of article 7 in certain cases (e.g., negotiable instruments).

43. It was widely felt that the main disadvantage of the proposed new article lied in the fact that, unlike article 7 of the Model Law and contrary to rules applicable in a paper-based environment, it allowed parties to derogate from mandatory rules of law. Thus, the proposed new article could inadvertently result in subverting the Model Law and national law relating to signatures and inappropriately affecting rights of third parties. In addition, there was broad support for the view that the proposed new article unnecessarily repeated elements contained in draft article 1 of the Uniform Rules.

44. In order to bring the proposed new article in line with article 7 of the Model Law and to address its above-mentioned deficiencies, a number of suggestions were made. One suggestion was to include a reference to the essential characteristics of a signature, namely those relating to identification of a person and approval of the contents of a message, by inserting at the end of the chapeau of paragraph (1) of the proposed new article language along the following lines: "is the signature of that person and". Another suggestion was to give precedence to applicable law by introducing at the beginning of paragraph (1)(a) language along the following lines: "subject to the relevant law". Yet another suggestion was that, in line with article 7 of the Model Law, the conjunction between subparagraphs (a) and (b) should be "and", and not "or". A further suggestion was that taking into account the conduct of the parties and relevant trade usages, as indicated in paragraph (2) of the new article, should be permitted rather than imposed, a result that could be achieved by replacing the word "shall" with the term "may". Yet another suggestion was that the essential elements of article 7(2) and (3) of the Model Law should be introduced in the proposed new article.

45. The view was widely shared that, instead of redrafting the proposed new article, the Working Group should attempt to establish basic principles regarding the extent to which party autonomy should be accommodated by the Uniform Rules. It was generally agreed that the Uniform Rules should not normally limit party autonomy as between the parties. It was also agreed that the efforts of the Working Group should be aimed at identifying the types of transactions (and, in the case of digital signatures, the types of certificates) that would imply a high level of security and might thus be subject to mandatory rules under existing law in a number of countries. With respect to the legal form requirements that were likely to interfere with party autonomy, it was widely felt that a useful distinction might be drawn between those requirements for signatures that were aimed at providing evidence (which might be made subject to party autonomy) and those form requirements that were prescribed for validity purposes (which would typically be mandatory).

46. After discussion, the Working Group requested the Secretariat to prepare a revised draft of article 1 taking into account the above deliberations and decisions.

Article 2. Presumptions

47. The text of draft article 2 as considered by the Working Group was as follows:

"(1) With respect to a data message authenticated by means of a secure electronic signature, it is rebuttably presumed that:

"(a) the data message has not been altered since the time the secure electronic signature was affixed to the data message;

"(b) the secure electronic signature is the signature of the person to whom it relates; and

"(c) the secure electronic signature was affixed by that person with the intention of signing the message.

"(2) With respect to a data message authenticated by means of an electronic signature other than a secure electronic signature, nothing in these Rules affects existing legal or evidentiary rules regarding the burden of proving the authenticity and integrity of a data message or an electronic signature.

"(3) The provisions of this article do not apply to the following: [...].

"[(4) The presumptions in paragraph (1) may be rebutted by:

"(a) evidence indicating that a security procedure used to verify an electronic signature is not to be generally recognized as trustworthy, due to advances in technology, the way in which the security procedure was implemented, or other reasons;

"(b) evidence indicating that the security procedure agreed to between the parties under article 1(c)(iii) was not implemented in a trustworthy manner; or

"(c) evidence relating to facts of which the relying party was aware which would suggest that reliance on the security procedure was not reasonable. The commercial reasonableness of a security procedure agreed upon by the parties under article 1(c)(iii) is to be determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agreed to adopt the procedure, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by the party, cost of alternative procedures, and procedures in general use for similar types of transactions.]"

48. While it was agreed that the principle of media neutrality should be reflected in the Uniform Rules through the recognition of the legal effects that would attach to the use of electronic signatures relying on non-digital techniques, the Working Group decided to defer its consideration of draft article 2 until it had completed its review of the remaining draft articles of the Uniform Rules.

Article 3. Attribution

49. The text of draft article 3 as considered by the Working Group was as follows:

"(1) Variant A Subject to [article 13 of the UNCITRAL Model Law on Electronic Commerce], the originator of a data message on which the originator's secure electronic signature is affixed is [bound by the content] [deemed to be the signer] of the message in the same manner as if the message had existed in a [manually] signed form in accordance with the law applicable to the content of the message.

Variant B As between the holder of a private key and any third party who relies on a digital signature which can be [verified] [authenticated] by using the corresponding certified public key, the digital signature [is presumed to be that of the holder] [satisfies the conditions set forth in [article 7(1) of the UNCITRAL Model Law on Electronic Commerce]].

"(2) Paragraph (1) does not apply if

"(a) the [originator] [holder] can establish that the [secure electronic signature] [private key] was used without authorization and that the [originator] [holder] could not have avoided such use by exercising reasonable care; or

"(b) the relying party knew or should have known, had it sought information from the [originator] [certification authority] or otherwise exercised reasonable care, that the [secure electronic] [digital] signature was not that of the [originator] [holder of the private key]."

General remarks

50. The Working Group first considered the purpose and scope of draft article 3 and its relationship with articles 7 and 13 of the Model Law.

51. Differing views were expressed as to whether the draft article should deal only with the attribution of secure electronic signatures (or digital signatures) or whether it should also address the issue of liability of the purported signer to the relying parties. One view was that draft article 3 should be aimed at linking a signature to the purported signer and at ensuring the integrity of a data message. Another view was that the main purpose of draft article 3 should be to create an incentive for the use of digital signatures by properly allocating liability for the loss caused to the relying party through the failure of the purported signer to exercise reasonable care and avoid the unauthorized use of its signature (see below, para. 58). The prevailing view was that both issues should be dealt with. In that context, a note of caution was struck about dealing with issues of liability, which might be inconsistent with the approach followed in the Model Law, under which contractual matters were left to the law applicable outside the Model Law. In response, it was observed that the Uniform Rules were based on a somehow different approach in that they already dealt, *inter alia*, with liability of certification authorities. After discussion, the Working Group agreed to consider dealing with both issues, possibly in separate provisions (see below, paras. 55 and 60).

52. With regard to the scope of draft article 3, the view was expressed that it should be limited to digital signatures and draft article 3 should be relocated accordingly. In support of that view, it was stated that digital signatures were so well known and widely used that they deserved to be given priority. In addition, it was stated that the issue of attribution of digital signatures was important enough to be treated separately from the issue of attribution of other types of electronic signatures. Another view was that the rules established under draft article 3 should apply both to digital signatures and to other electronic signatures. The prevailing view was that, to the extent possible, the issues addressed under draft article 3 should be dealt with in a media-neutral manner to cover a broad range of electronic signatures.

53. As to the relationship between draft article 3 and articles 7 and 13 of the Model Law, it was observed that article 7 dealt with requirements for signatures and article 13 with attribution of messages. A concern was expressed that draft article 3 might merely restate the provisions of article 13 of the Model Law. In response, it was stated that draft article 3 dealt with the attribution of an electronic signature as distinct from the attribution of the data message and provided specific protection to the purported signer in cases where its signature was used without authorisation and the purported signer could not have avoided such unauthorised use, had it exercised reasonable care.

Paragraph (1)

54. Support was expressed in favour of both Variants A and B. In favour of Variant A, it was stated that it was based on a media-neutral approach, and thus addressed different types of technologies used in international trade. In that connection, it was pointed out that neutrality should be ensured also as to the way in which a particular technology was being implemented (e.g., a digital signature with or without a certificate). Such implementation neutrality could be obtained, it was observed, through a general rule to the effect that the recipient of the data message who reasonably relied on a secure electronic signature would be entitled to regard that message as being that of the purported signer (see A/CN.9/WG.IV/WP.73, paras. 35-36). In support of Variant B, it was said that it appropriately focused on digital signatures which, by contrast to other types of electronic signatures, were sufficiently known and widely used.

55. However, both Variants A and B were criticized for inappropriately mixing two different issues, namely the issue of attribution and the issue of liability. In addition, a number of concerns were expressed and observations were made with regard to both Variants. As to Variant A, it was observed that: the opening words were not sufficiently clear; use of the term "originator" was not appropriate for a number of reasons, including that the signer of a data message did not necessarily have to be its originator; the words "is bound by the content" related to the general law of obligations and not to the mere attribution of electronic signatures to the purported signer; and the reference to the law applicable should relate to the law applicable to the data message as a whole and not only to its contents.

56. As to Variant B, it was observed that: in order to avoid overriding the exceptions set forth in other provisions of the Uniform Rules relating, e.g., to compromised private keys, language should be added at the beginning of Variant B along the following lines "subject to the provisions of articles ..."; in line with the approach taken in article 13 of the Model Law, reference should be made to actual verification of the authenticated use of a digital signature, and not merely to the ability of the holder of the private key to verify such use; in order to avoid a situation in which a digital signature could be attributed to the purported signer, even though the certificate had been revoked, language along the following lines should be used "private key contained in a valid certificate"; no reference should be made to article 7 of the Model Law, since that article dealt with the requirement for a signature and not with attribution of a signature.

Paragraph (2)

57. While there was agreement in the Working Group that paragraph (2) was generally acceptable, the concern was expressed that use of the term "reasonable care" might introduce uncertainty. In order to address that concern, a number of suggestions were made. One suggestion was that the signature should be attributed to the purported signer if it failed to establish that the use of the signature was unauthorized. Another suggestion was that the signature should be deemed to be that of the purported signer if, in addition, it failed to establish that it could not have avoided the unauthorized use, without any reference being made to the notion of "reasonable care". Both suggestions were objected to on the ground that they would inappropriately increase the level of responsibility of the purported signer.

Suggestions for a new article 3

58. In order to address the concerns expressed with regard to draft article 3 and on the assumption that the issue of attribution of secure electronic signatures was sufficiently addressed in draft article 2 of the Uniform Rules, the suggestion was made that the focus of draft article 3 should be shifted to the issue of liability of the purported signer and, thus, article 3 should read along the following lines:

> "(1) As between the holder of a private key and any person relying on a digital signature, the holder is not bound by the message if he did not sign it.
>
> "(2) If the key holder has not exercised reasonable care to prevent the relying party from relying on the unauthorized use of the digital signature, he is liable to compensate the relying party for harm caused to him. The relying party is only entitled to such compensation if he had sought information from the certification authority or otherwise exercised reasonable care to establish that the digital signature was not that of the holder."

59. While it was generally agreed that the suggested language rightly distinguished between attribution of a signature and accountability (or liability) for harm caused by the unauthorized used of a signature, it was observed that it did not sufficiently address the concerns expressed with regard to Variants A and B. In addition, it was observed that it shifted the burden of proof against the relying party who had to establish that it used reasonable care in order to prove that the signature was that of the purported signer. It was generally agreed that a media-neutral approach would be preferable, and that the issues of attribution and accountability should be dealt with separately.

60. With a view to reflecting that approach, the Working Group was invited to consider an alternative formulation along the following lines:

> "Attribution of secure electronic signatures
>
> "As between the purported signer and the relying party, a secure electronic signature is deemed to be that of the purported signer, unless the purported signer can establish that the secure electronic signature was used without authorisation.
>
> "Liability for secure electronic signature
>
> "In a case where the secure electronic signature was unauthorised and the purported signer did not exercise reasonable care to prevent the addressee from relying on such a message, the purported signer is liable to pay damages to compensate the relying party for harm caused, unless the relying party did not seek information from an appropriate third party or otherwise knew or should have known that the signature was not that of the purported signer."

61. After discussion, the Working Group requested the Secretariat to reflect the suggested alternative formulation in a revised draft of the Uniform Rules for further consideration by the Working Group at a future session. A concern was expressed by a number of delegations about possible interference between the suggested formulation and their domestic tort law.

Section II . Digital signatures

Article 4. Definition

62. The text of draft article 4 as considered by the Working Group was as follows:

"For the purposes of these Rules,

"Variant A 'digital signature' means a type of an electronic signature consisting of a transformation of a data message using a message digest function and an asymmetric cryptosystem such that any person having the initial untransformed data message and the signer's public key can accurately determine:

"(a) whether the transformation was created using the signer's private key that corresponds to the signer's public key; and

"(b) whether the initial data message has been altered since the transformation was made.

"Variant B "(a) 'digital signature' means a numerical value, which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine that this numerical value has only been obtained with the originator's private key;

"(b) The mathematical procedures used for generating digital signatures under these Rules are based on public-key encryption. When applied to a data message, those mathematical procedures operate a transformation of the message such that a person having the initial message and the originator's public key can accurately determine:

"(i) whether the transformation was operated using the private key that corresponds to the originator's public key; and

"(ii) whether the initial message was altered after the transformation was made."

63. While some support was expressed in favour of both Variants A and B, neither one was adopted by the Working Group.

64. In favour of Variant A, it was stated that, to the extent it focused on the creation of a digital signature without referring to any specific technology, it was sufficiently flexible to encompass different types of digital signatures. However, a concern was expressed that Variant A failed to recognize the different ways in which a public key infrastructure might be implemented (e.g., with or without reliance on a message digest function), and the different functions that might be fulfilled through the use of a digital signature (e.g., the function of identifying the signer ("secure signatures"), the function of establishing the integrity of the data message ("secure records"), or a combination of both functions). In the context of that discussion, it was suggested that, in order to ensure cross-border recognition of different types of digital signatures and certificates, consideration should be given by the Working Group to the idea of preparing a convention instead of an addition to the Model Law (see below, para. 212).

65. In response to the above-mentioned concern, it was observed that it was a well-established approach to include the elements of identification of the signer and verification of the message integrity in a definition of "digital signature". In addition, it was pointed out that that approach, which was aimed at identifying a functional equivalent of a signature in a paper-based context, was in line with the approach taken in the Model Law. Moreover, it was stated that an effort to address all types of digital signatures would be overly ambitious and would delay progress in a field which needed urgent regulation so that disharmony of law through the introduction of different approaches in national legislation might be avoided. In that regard, it was observed that Variant A, by defining digital signature as a type of electronic signature, would confine that term to those applications of public-key cryptography that were meant to serve as a functional equivalent of a signature in a paper-based context, whereas Variant B would be wide enough to cover all manifestations of digital signature technology, including those that were not meant to serve as functional equivalents of signatures.

66. In favour of Variant B, it was observed that it introduced more certainty as to the scope of the provision in that it was stated in more technical terms and specifically referred to public-key encryption, which was said to constitute a widely-used technology. At the same time, the concern was expressed that Variant B was too restrictive to the extent that it relied on a certain mathematical procedure for the creation of a digital signature, thus possibly excluding future technical developments that might render currently accepted procedures obsolete. It was suggested that a reference to "state-of-the-art mathematical procedures" might need to be made in the draft provision.

67. Both Variants A and B were objected to on the grounds that they inappropriately defined "digital signature" by reference to "a transformation of the data message". It was explained that it was not the message as a whole, but only its numerical representation that changed as a result of processing the message through the use of an algorithm. In order to address that problem, language along the following lines was proposed:

> "Digital signature is a cryptographic transformation (using an asymmetric cryptographic technique) of the numerical representation of a data message, such that any person having the data message and the relevant public key can determine:

"(a) that the transformation was created using the private key corresponding to the relevant public key; and

"(b) that the data message has not been altered since the cryptographic transformation."

68. In support of the proposed text, it was stated that, by avoiding to refer to the signer's private key, it addressed the need to ensure that digital signatures used for various purposes, beyond identification of the signer, would be covered by the Uniform Rules. It was also stated that, by avoiding reference to a message digest function, the proposed text would also cover digital signatures created through a different procedure.

69. During the discussion, the suggestion was made that the Working Group should consider, merely for purposes of comparison, the text adopted in 1988 by the International Standards Organization (ISO), which read as follows: "Digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient" (ISO 7498-2). Another suggestion was that the ISO definition should be included in the Uniform Rules. While it was agreed that the ISO definition demonstrated a technical approach, there was widely shared skepticism in the Working Group as to whether that definition was suitable for the purposes of the Uniform Rules.

70. After discussion, the Working Group generally agreed that it should reserve its decision as to the definition of "digital signature" until it had completed its review of the substantive provisions of the Uniform Rules and come to a conclusion as to the scope of those provisions. In particular, the definition of "digital signature" might vary depending on whether the Uniform Rules covered only the uses of computer-based techniques which were aimed at replicating in an electronic environment the functions traditionally fulfilled through the use of hand-written signatures in international trade transactions, or whether the scope of the Uniform Rules was extended to cover additional uses of "digital signatures". The Secretariat was requested to prepare alternative drafts based on Variants A and B, and on the above-mentioned proposal (see above, para. 67), taking into account the comments made, for further consideration of the matter at a future session.

Article 5. Effects

71. The text of draft article 5 as considered by the Working Group was as follows:

"(1) Where all or any portion of a data message is signed with a digital signature, the digital signature is regarded as a secure electronic signature with respect to such portion of the message if:

"(a) the digital signature was created during the operational period of a [valid] certificate and is verified by reference to the public key listed in the certificate; and

"(b) the certificate is considered as accurately binding a public key to a person's identity because:

"(i) the certificate was issued by a certification authority licensed [accredited] by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

"(ii) the certificate was otherwise issued by a certification authority in accordance with standards issued by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*.

"(2) Where all or any portion of a data message is signed with a digital signature that does not meet the requirements set forth in paragraph (1), the digital signature is regarded as a secure electronic signature with respect to such portion of the message if sufficient evidence indicates that the certificate accurately binds the public key to the holder's identity.

"(3) The provisions of this article do not apply to the following: [...]."

General remarks

72. It was widely recognized, at the outset, that the substance of draft article 5 would need to be further discussed by the Working Group in the light of the decisions to be made as to the scope of the Uniform Rules. In particular, draft article 5 was directly dependent upon whether the notion of "secure electronic signature" would eventually be used in the Uniform Rules. The legal effects attached to the use of certificates in the context of digital signatures would also depend upon the definition of "certificate" under draft article 8. Should the Uniform Rules cover only the cases where digital signatures were used for the purposes of international trade transactions with the intent to sign (i.e., to identify the signer and link the signer with the information being signed), it might be acceptable to limit the function of the certificate to linking a key pair with the identity of a person. In such a case, it should be specified that the Uniform Rules were dealing only with a special kind of certificates ("identity certificates"), particularly since other types of certificates might be used in electronic commerce, e.g., to establish the level of authority of a person ("authority certificates"). A view was expressed that authority certificates should be covered by draft article 5 together with identity certificates. In the context of that discussion, it was suggested that a reference should be made in draft article 5 to the certificate verifying the integrity of the information contained in the data message. In response, it was stated that, while verification of data integrity was an important result of the use of the certificate in the context of a digital signature process, it was not a characteristic element of the certificate itself.

73. After discussion, the Working Group decided to proceed with its consideration of draft article 5. It was generally agreed, however, that the discussion would need to be reopened after the Working Group had completed its review of the substantive provisions of the Uniform Rules.

Title

74. A widely shared view was that the title of draft article 5 was insufficiently descriptive and might be misleading. It was decided that the title should be reworded along the following lines: "Digital signatures supported by certificates".

Paragraph (1)

Opening words

75. Support was expressed in favour of the view that the reference to the notion of "secure electronic signature" was not necessary in draft article 5 and should be replaced by a reference to the conditions set forth in article 7 of the Model Law. It was stated in response that such a reference to article 7 of the Model Law would inappropriately limit the scope of the draft article 5 by presupposing the existence of legal requirements for a signature, which would need to be met in an electronic environment. The purpose of draft article 5 was broader and directly aimed at creating certainty as to the legal effects of digital signatures, provided that certain technical standards were met, irrespective of whether there existed a specific requirement for a signature.

76. After discussion, the Working Group decided that references to a "secure electronic signature" and to the conditions set forth in article 7 of the Model Law should be kept as alternative wordings for further consideration by the Working Group at a future session. The opening words of draft article 5 should read along the following lines: "In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature [is a secure electronic signature][satisfies the conditions in article 7 of the UNCITRAL Model Law on Electronic Commerce] if".

Subparagraph (a)

77. The substance of subparagraph (a) was found to be generally acceptable. With a view to better reflecting the necessary trustworthiness of the digital signature process, it was decided that the word "securely" should be inserted to qualify both the creation of the digital signature and its verification by reference to the public key listed in the certificate. It was also decided that the reference to the validity of the certificate should be maintained without square brackets in the draft provision.

Subparagraph (b)

78. With respect to subparagraph (b)(i), it was widely felt that the words "licensed" or "registered" were preferable to the word "accredited" in a provision dealing with the case where States would adopt a regulatory approach to public-key infrastructures. As regards subparagraph (b)(ii), the view was expressed that the provision should be deleted, since the scope of draft article 5 should be limited to the use of certificates issued by certification authorities licensed by the enacting State. The prevailing view, however, was that a reference should be made to industry

standards and to mechanisms that might be developed by practitioners to ensure the reliability of such standards. It was generally agreed that such a reference was necessary to reflect the "dual approach" to digital signatures and public-key infrastructures adopted by the Working Group at its previous session (see A/CN.9/437, para. 69). Under that approach, industry-based standards would be recognized alongside government regulation. It was pointed out that, in certain countries, government authorities might wish not to become involved with the establishment of security standards for digital signatures. In that connection, it was stated that draft article 5 should not only mention "security standards" but cover more broadly the various types of standards that might be developed by the industry.

79. With respect to the reference to recognized industry standards, it was suggested that wording might be drawn from article 9(2) of the United Nations Convention on Contracts for the International Sale of Goods, which referred to "a usage of which the parties knew or ought to have known and which in international trade is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade concerned". It was widely felt, however, that a reference to "commercially appropriate and internationally recognized standards" would be more appropriate.

80. Taking into account the above-mentioned discussion, it was agreed that subparagraph (b) should be redrafted along the following lines for the purpose of future discussion:

"(b) the certificate binds a public key to a person's identity by virtue of the fact that:

"(i) the certificate was issued by a certification authority licensed by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

"(ii) the certificate was issued by a certification authority accredited by a responsible accreditation body applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics. A non-exclusive list of bodies or standards that comply with this paragraph may be published by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*; or

"(iii) the certificate was otherwise issued in accordance with commercially appropriate and internationally recognized standards."

Paragraph (2)

81. A number of concerns were expressed in connection with paragraph (2). One concern was that paragraph (2) might be redundant in the light of draft article 2, which set forth the legal presumptions attached to the status of a "secure electronic signature". In response, it was stated that paragraph (2) was necessary to establish the link between a digital signature that might be

recognized (e.g., by a court of justice) as binding the public key to the holder although it did not formally meet the requirements set forth in paragraph (1), and other provisions of the Uniform Rules (e.g., revised draft article 3 on "liability for secure electronic signature"). In that context, the view was expressed that the words "Notwithstanding the provisions of article 5" might have to be introduced in draft article 3.

82. Another concern was that paragraph (2) established an excessively low standard for the recognition of digital signatures that did not otherwise meet the requirements set forth in paragraph (1). As currently drafted, paragraph (2) might lead to granting a "secure" status to digital signatures which relied on insecure procedures, e.g., for lack of sufficient key length. In response, it was stated that, while additional reference to the trustworthiness of the technical procedures might need to be introduced either in draft article 5 or in the definition of "secure electronic signature", a provision along the lines of paragraph (2) was necessary to preserve the possibility that parties might be allowed to establish before a court or an arbitral tribunal that the digital signature they used was sufficiently reliable to be granted legal value although it was used outside the context of paragraph (1). However, a concern was expressed that the granting of "secure" status created presumptions and assigned tort liabilities under draft articles 2 and 3. It was stated that such serious consequences should be ascertainable by reference to clear rules and standards before the signature was used, instead of being imposed on an unsuspecting party by a court at a later stage.

83. Various suggestions were made as to how the reference to the general rules of evidence contained in paragraph (2) should be expressed. One view was that paragraph (2) should be broader in scope, to encompass not only the situation where a certificate was used but also any other situation where a digital signature or any other electronic signature was used. Under that view, the reference to "the certificate" should be deleted from paragraph (2), which should be relocated in the section dealing with electronic signatures in general. Another view was that the scope of paragraph (2) should be narrower and the provision should apply only where the digital signature was created during the validity period of a certificate. Under that view, the rule contained in paragraph (2) should be made part of paragraph (1)(b) along the following lines:

> "(iv) sufficient evidence indicates that the certificate accurately binds the public key to the holder's identity."

84. After discussion, the Working Group did not reach consensus as to the scope and placement of the provision contained in paragraph (2). The Secretariat was requested to prepare a revised draft provision, with variants reflecting the discussion for consideration by the Working Group at a future session.

Article 6. Signature by legal persons

85. The text of draft article 6 as considered by the Working Group was as follows:

> "[A legal person may identify a data message by affixing to that message the public cryptographic key certified for that legal person. The legal person shall only be regarded as [the originator][having approved the sending] of the message if the message is also digitally signed by the natural person authorized to act on behalf of that legal person.]"

86. It was recalled that, at the previous session of the Working Group, it had been widely felt that draft article 6 should be deleted. It had been kept between square brackets as a reminder that the Working Group might need to discuss more fully the extent to which the Uniform Rules should validate the operation of "electronic agents" for the purpose of automatically authenticating data messages (see A/CN.9/437, paras. 115-117). The Working Group decided that the question of "electronic agents" would need to be discussed at a later stage. It was decided, however, that draft article 6 should be deleted, since it might be seen as inappropriately interfering with other bodies of law (e.g., the law of agency, and the provisions of company law dealing with representation of companies by natural persons).

Section III. Other electronic signatures

87. There was general agreement that Section III should remain in the Uniform Rules, pending a decision as to whether the principle of non-discrimination embodied in the definitions of "signature" and "secure electronic signatures" (and expressed through the legal status recognized to any authentication technique that would qualify as a "secure" electronic signature) should also be expressed by way of more specific provisions dealing with authentication techniques other than digital signatures.

88. With a view to providing more information to the Working Group as to how digital signatures and various other authentication techniques might operate, a number of presentations of a technical nature were made. Those presentations are summarized below (paras. 89 to 105).

89. It was recalled that secure electronic commerce required that parties to a transaction have the ability to authenticate each other. In many instances of electronic interaction (e.g. shopping on the Internet), traditional methods of authentication were either unavailable or unreliable. This need for reliable methods of electronic authentication extended beyond the requirements of commerce into nearly every type of interaction in a digital world.

90. It was pointed out that a wide variety of solutions were currently available to address these needs. These solutions had both a technological and a methodological component. While much of the focus tended to be on the differing technological approaches, the impact of the methodology or business model underlying the electronic authentication solution should not be underestimated. In addition to the many different technological approaches, the market had also provided a rich variety of methodologies implementing these technologies. This diversity of solutions reflected the

different types of authentication required by the many different situations presented in a digital environment. As this environment developed, new authentication solutions would be required.

91. Methods of authentication could be categorized by focusing on the characteristic being authenticated. The three basic categories of characteristics were described as: (1) "something you know"; (2) "something you are"; and (3) "something you have". Many solutions used a combination of these three characteristics.

92. The first category ("something you know") was one of the most commonly used characteristics to authenticate individuals. Passwords, pass phrases and personal identification numbers (PINs) fell into this category. Most computer systems provided password options that allowed access to resources to those that had a valid password. For example, automated access to bank account informa' on required users to know the correct PIN associated with the account being queried. Another type of authentication in this category was based upon personal information that only a specific individual was likely to know. For example, in some jurisdictions, it was common for a bank to ask an individual to provide his or her mother's birth surname when setting up a bank account. This information could be used at a later date to authenticate the account holder. While this category of authentication was widely used in current practice, it had a number of weaknesses. First, it usually required that the shared knowledge be either secret or difficult to obtain. Second, it required that the parties have a pre-existing relationship where they could "share" the secret element of knowledge (e.g. password, PIN or mother's birth surname).

93. The second category of authentication methods ("something you are"), was often referred to as biometrics. This approach used innate qualities of the individual for authentication. Some of the innate aspects used in biometrics included: fingerprints, retinas, irises, hand-prints, voice prints, and handwritten signatures. Since all of these characteristics were unique to individuals, they provided an excellent method for authentication. If information about these characteristics could be made publicly available, then this type of authentication would not require a pre-existing relationship. Additionally, these approaches could often provide strong authentication because manipulating or tricking these systems was very difficult. One down side of these approaches was that they involved a higher cost of implementation since they required some type of hardware to be used to obtain information about the aspect in question. Another concern with some applications in this category was the device used to collect the biometric information. In some cases the devices were considered obtrusive (e.g., the retina scanner required users to place their eye up to an eyepiece where a red light was used to scan the retina). In other cases, information obtained in the authentication scan could divulge personal health information that the individual did not want to make public (e.g., certain health conditions could be diagnosed by irregularities in the iris, therefore, while the iris scan was not as physically obtrusive, it was considered by some to be personally invasive). Finally, some of these devices were not always reliable if the conditions of use were "abnormal" (e.g., fingerprints with a cut on a finger). Nonetheless, biometric solutions were widely considered one of the strongest methods of authentication and were currently being used in practice. Examples were given of a country where the immigration and naturalization services were testing a hand-print technology solution to speed up passport control, and of insurance companies that were using signature biometrics to authenticate individuals in claims processing.

94. The third category of authentication methods ("something you have") was described as one of the most active areas in electronic authentication. The "something" could be physical (e.g., a challenge-response device) or it could be information (e.g., an encryption key). A challenge-response device was similar to the shared secret approach used in the "something you know" category, only it was implemented in hardware. This solution required individuals to be given a device that was unique and was assigned to that individual user only. When the individual attempted to access a service, the host system asked the persons to identify themselves (usually by way of a user name) and then the system generated a numeric challenge based upon the information the system had about the unique device assigned to the individual. The individual then keyed that number into the device, which generated a numeric response. That numeric response could then be keyed into the system to which the holder of the device was trying to gain access . The host system "knew" that there was only one acceptable response to the numeric challenge it presented to the individual and that acceptable response could only be generated by the unique device assigned to the individual. Therefore, if the individual typed in the proper numeric response, then the host system "knew" that the person attempting to gain access was who that person claimed to be. That type of device was commonly used in authenticating individuals that sought remote access to computer systems. It was also being used by a bank in a home banking pilot project referred to as "browser banking" because it allows an individual access to the bank account from any browser on any machine. This application demonstrated one of the strengths of the approach. For while it did require a hardware component, it did not require a system modification like that required by chip cards.

95. The other subcategory of the third category covered the use of digital signatures. The important aspect of digital signature technology was the use of a private key to generate a digital signature and the use of a public key to authenticate the digital signature. The private key used to generate the digital signatures could be stored on a hard disk or on a smart card and had to be kept very private by the person using it. The public key was disseminated widely. There were several different paradigms for using digital signature technology, each having a different way of providing trust to the recipient of a digital signature.

96. One of the first approaches was to create a directory of individuals and public keys. Under this model, the recipient of a digitally-signed document verified the public key of the signer of the document by looking up the public key in a trusted directory. It was reported that a number of applications currently used this model.

97. Another approach, historically developed from the directory-based approach, relied on the use of digital certificates. Digital certificates were electronic documents digitally signed by a trusted entity. When a document was digitally signed, a copy of the digital certificate of the signer was attached. It contained information about the individual and the individual's public key. When the recipient received the message and the digital certificate, the recipient used the public key in the digital certificate to authenticate the message.

98. One common use of digital certificates employed a standard (ISO X.509), which allowed for a hierarchy of trusted entities to be used to authenticate parties. This approach was often referred to as the credit card model, as it reflected the business model underlying the credit card industry. For

example, a merchant might not know a consumer, but it was willing to accept a certain card for payment, because the merchant knew that the card was issued to the consumer by a bank (the bank's name was always on the card), which was authorized to issue that card by the credit card company. Even if the merchant did not know the bank that issued the card, it could trust the consumer because it knew that the consumer has been authenticated by the bank and the bank has been authenticated by the credit card company. Similarly, X.509 trust hierarchies allowed digital certificates to be authenticated by a hierarchical chain of trusted entities (called "Certificate Authorities" and otherwise referred to in this report as "certification authorities") that could be verified by the recipient of the certificate. The last certification authority in this trust tree was known as the root. Therefore, digitally signing a document in the X.509 approach, involved sending the signer's digital certificate and all of the supporting digital certificates associated with the trust hierarchy being relied upon. Under that model, the recipient could verify the entire trust tree without having to check an online directory. This approach was described as especially well-suited for enabling trusted communications amongst large numbers of people who might have little or no prior contact with each other. One of the strengths of this approach, the ability to relate many certificates back to a trusted root, was also one of the weaknesses. If this root was compromised, everything beneath the root became unreliable.

99. Another variant of the use of digital certificates was commonly referred to as the web of trust model. In this model, there were no certification authorities. Digital certificates were generated by individuals. There was no trusted root. Individuals decided who they would trust and how much. This model was designed for small communities of users who had regular contacts, and was difficult to implement on large scales. Nonetheless, this model was currently being used in many environments.

100. It was stated that an important consideration in understanding the use of X.509 digital certificates was the historical bias towards identity. Since the X.509 standard arose out of the X.500 directory, it was naturally focused on associating public keys with the identity of individuals. This pre-disposition with identity was said to confuse many public policy questions surrounding the use of the digital signatures. While it was clear that certain digital certificates authenticated the identity of a person, it is equally clear that other digital certificates had functions other than authenticating identity. Digital certificates could also be used to authenticate an individual's rights or relationships without making any statement about the individual's identity. In many cases, the individual's identity was unnecessary or even undesirable. There were many special-purpose certificates that could only be used for certain functions just like an individual's credit card could not be used to authenticate the individual's identity and an individual's passport could not be used to purchase goods. The inclination to think in terms of identity, while logical, could severely limit the use of the technology. If every application that used digital signatures needed to fulfil the strict requirements of a general-purpose identity certificate, then the technology would be very difficult and expensive to use. It was important to remember that there would be a broad spectrum of authentication requirements and the technology was sufficiently flexible to meet all of these requirements.

101. When a number of credit card companies decided to develop a secure method for electronic commerce over public networks like the Internet, they identified three primary business objectives:

the solution had to be secure; the solution had to be open to any technology supplier interested in developing a product that complied with the defined protocol; and all implementations must be inter-operable. For the payment industry, "secure" has the following three components: (1) the privacy of the payment information, including consumer's account number; (2) the integrity of the order information; and (3) authentication of the parties to the transaction. Aimed at providing the required level of "security", the Secure Electronic Transaction ("SET") protocol was created. This protocol used digital signatures (based on the X.509 model) to fulfil the data integrity and party authentication function.

102. A brief description of the SET protocol was made. A consumer who decided to engage in secure electronic commerce with SET had first to obtain software that has passed the compliance procedures set forth by the SET Root certification authority. This software generated a key pair and an application that the consumer sent to the entity that issued the payment card intended for use. The software put the public key into the certificate application and prompted the consumer to provide identifying information so the financial institution can verify that the person requesting the certificate was authorized to do so. This application was sent to the financial institution through the Internet. If the application was accepted, the financial institution digitally signed the consumer's certificate and sent it back to the consumer via the Internet. The consumer's software stored this digital certificate on the consumer's computer. This application procedure was only done once to obtain the certificate.

103. The consumer then started to shop online and could initiate secure transactions with merchants using SET-compliant software. In the first stages of the transaction, the consumer's software requested authenticating information from the merchant. The software authenticated the merchant by verifying all of the digital signatures and digital certificates sent by the merchant. If there was a failure at any point in the authentication process, the consumer was warned. The consumer then identified the goods or services to be purchased, selected the payment method and initiated the transaction. The consumer software separated the payment information from the order information. The payment information was encrypted using strong cryptography so that the financial institution of the merchant was the only one that could decrypt the payment information. The order information, which specified what was to be purchased and other details of the transaction, and the encrypted payment information was digitally signed and sent to the merchant. When the merchant received this message, it would separate the encrypted payment information, digitally sign this new message and send it to its financial institution. The financial institution would verify the digital signature of the merchant, decrypt the payment information and then submit the payment information for processing through the existing payment infrastructure. The financial institution digitally signed the authorization response and sent it to the merchant. The merchant then sent a digitally-signed response to the consumer. If the transaction was authorized, the merchant fulfilled the order.

104. SET was said to illustrate reliance upon digital signature technology in authenticating messages and parties. However, it was important to note that the SET certificates were not identity certificates. They did not authenticate anyone's identity, nor could they be used for that function, as explicitly provided in the policy statement associated with the certificates. SET certificates merely authenticated the relationship of a public key to an account number. SET used digital

signature technology to provide extra security to the transaction, not to identify an individual. Furthermore, SET did not use certificate revocation lists ("CRL") for consumer or merchant certificates. In the context of the SET business model, such lists were not necessary. Transactions were still required to be authorized through the existing payment infrastructure, so the addition of a cardholder CRL would provide no benefit while adding significant costs in the construction and maintenance of the system.

105. SET was said to illustrate: (1) non-identity use of digital signatures and certificates; (2) issuance of certificates by non-licensed, market-based certification authorities; (3) issuance of certificates within a system where parties had defined their rights and responsibilities by agreement; and (4) that in some instances a relying party (the bank who completed the payment based on information digitally signed by the consumer) might be the issuer of the certificate. SET was just one example of an implementation of digital signature technology. It was stated that there would be many other uses in the coming years and they would be based on technologies and business models that had yet to emerge.

106. The Working Group expressed its appreciation for the presentations that were made. It was generally felt that illustrations of the techniques being implemented or considered for implementation were helpful to better understand the legal issues that needed to be addressed in the Uniform Rules. The Working Group expressed the hope that further presentations on developments in digital signature and other authentication techniques could be made in the context of its future sessions.

CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES

Article 7. Certification authority

107. The text of draft article 7 as considered by the Working Group was as follows:

"(1) For the purposes of these Rules, "certification authority" means:

"(a) any person or entity licensed [accredited] by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]* to act in pursuance of these Rules; or

"(b) any person who, or entity which, as an ordinary part of its business, engages in issuing certificates in relation to cryptographic keys used for the purposes of digital signatures.

"[(2) A certification authority may offer or facilitate registration and time stamping of the transmission and reception of data messages as well as other functions regarding communications secured by means of digital signatures.]"

Paragraph (1)

108. The view was expressed that paragraph (1) placed too much emphasis on the situation where the function of a certification authority was performed by an independent third party (often referred to as a "trusted third party"), which was not the only conceivable situation. It was pointed out that in digital signature practice, parties relied increasingly on self-certification (or mutual-certification) schemes, involving only the originators and addressees of digitally-signed messages. Accordingly, the definition of "certification authority" should be broadened to cover all types of practices. It was suggested that the words "as an ordinary part of its business" in paragraph (1)(b) should be replaced by the words "in the course of its business". That suggestion was found to be generally acceptable.

109. Another suggestion was that, alongside the definition of "certification authority", the Working Group might need to address the definition of "registration authority". While no support was expressed in favour of that suggestion, it was generally felt that the issue might need to be discussed further at a later stage.

110. Yet another suggestion was that subparagraph (a) should be deleted, since it merely addressed a subset of the category dealt with under subparagraph (b). In support of that suggestion, it was stated that any reference to "licensed certification authorities" in the Uniform Rules might be interpreted as encouraging enacting States to establish licensing schemes, which might run counter to the "dual approach" adopted by the Working Group at its previous session (see A/CN.9/437, para. 69). It was also stated that the deletion of subparagraph (a), while preserving the necessary flexibility, would appropriately focus the Uniform Rules on the use of digital signatures for the purposes of international trade transactions, as opposed to the use of digital signatures for administrative purposes. The prevailing view, however, was that the substance of subparagraph (a) should be retained. It was stated that, in certain contexts, licensed certification authorities might not operate a "business". Moreover, the distinction between licensed certification authorities and those certification authorities that operated on a purely private basis was justified to reflect the different legal regimes that might affect the two types of certification authorities. As an example of such a difference, it was stated that antitrust legislation that might apply to privately-operated certification authorities might not apply to certification authorities performing public functions. Furthermore, even if the category dealt with under subparagraph (a) were encompassed in the provision contained in subparagraph (b), subparagraph (a) would still serve a useful purpose in that it would accommodate the needs of those States that intended to rely on a licensing scheme, thus preserving the neutrality of the Uniform Rules.

111. Taking into account the above discussion, it was decided that paragraph (1) should be redrafted along the following lines for the purpose of future discussion:

> "(1) For the purposes of these Rules, "certification authority" means any person who, or entity which, in the course of its business, engages in issuing certificates in relation to cryptographic keys used for the purposes of digital signatures.
>
> "(2) Paragraph (1) is subject to any applicable law which requires a certification authority to be licensed, to be accredited, or to operate in a manner specified in such law."

Paragraph (2)

112. Some support was expressed in favour of the retention of paragraph (2). The view was expressed that the various functions listed in paragraph (2) should be complemented by an express reference to other functions, such as the creation, management, suspension and revocation of certificates, to better illustrate the link between the various ancillary services offered by certification authorities and the operation of a digital signature system, which constituted the main activity of a certification authority. The widely prevailing view, however, was that paragraph (2) should be deleted and that its substance might be considered at a later stage for possible inclusion in a guide to enactment, should the Working Group eventually decide that such a guide should be prepared.

Article 8. Certificate

113. The text of draft article 8 as considered by the Working Group was as follows:

"For the purposes of these Rules, "certificate"means a data message [or other record] which, at least:

"(a) identifies the certification authority issuing it;

"(b) names or identifies its holder or a device or electronic agent under the control of the holder;

"(c) contains a public key which corresponds to a private key under the control of the holder;

"(d) specifies its operational period [and existing restrictions, if any, on the scope of use of the public key]; and

"(e) is [digitally] signed by the certification authority issuing it."

General remarks

114. It was generally agreed that draft article 8 should be divided into two parts (or into two separate articles), one that would contain a general definition of certificates to be covered in the Uniform Rules and another that would list the minimum contents of such certificates along the lines of subparagraphs (a) to (e). It was pointed out that such an approach could result in properly broadening the scope of the Uniform Rules, which would be more limited if all the elements contained in draft article 8 were part of the definition of "certificate".

Definition of "certificate"

115. At the outset, it was agreed that use of technical definitions of certificates might not be appropriate, since they were likely to be revised to address changing needs and technologies. The Working Group went on to consider a definition of "certificate", on the basis of language along the following lines: "For the purposes of these rules, "certificate" means a data message or other record issued by a certification authority for the purpose of identifying a person or entity who holds a private key".

116. It was pointed out that such a definition covered only identity certificates and left outside the scope of the Uniform Rules a variety of certificates that were widely used and might need to be recognized. In that regard, differing views were expressed. One view was that only identity certificates should be covered in the Uniform Rules. Another view was that other types of certificates (e.g., authority certificates) should be covered as well. While some support was expressed in favour of that view, a concern was expressed that, if other certificates were to be covered, the provisions dealing with the representations made by a certification authority and, as a result, its liability, would need to establish different legal regimes to cover the various types of certificates issued, which might result in an overly ambitious task for the Working Group.

117. As a matter of drafting, it was suggested that, in order to cover various types of certificates, a general definition might be prepared to cover all types of certificates, while the specific purpose of each type of certificate would be set forth in subsequent provisions. In order to reflect that approach, language along the following lines was proposed: "For the purposes of these rules, "certificate" means a data message that enables the verification of a data message corresponding to the public key contained in the certificate". Then, the purpose of each type of certificate would be set forth, e.g., along the following lines: "An identity certificate is intended to provide evidence of identity". Alternatively, it was suggested that, in order to reflect the idea that certificates might fulfil various functions, the definition would need to be amended to refer to a data message "which purports to verify the identity or other significant characteristic of a person". It was further suggested that the word "confirm", "establish", or other similar term should be substituted for the word "verify", which might sometimes be given a specific technical meaning.

118. The discussion focused on the latter suggested definition. As to the exact formulation of the definition of "identity certificate", a number of suggestions were made. One suggestion was that reference to "other records" should be avoided. In support of that suggestion, it was stated that introducing a reference to "records" in the Uniform Rules might create problems of interpretation of article 2(a) of the Model Law. In response, it was observed that such a reference to "records" would help avoid creating any uncertainty as to whether a certificate in a purely paper form would be covered by the Uniform Rules. Another suggestion was that, in order to avoid raising interpretation problems as to the subjective intentions of the parties, the words "for the purpose of identifying" should be replaced by the words "which identifies".

119. The suggested wording was objected to on the grounds that it might create a situation in which the certification authority would be able to escape liability by not identifying the person to whom the certificate was issued. Accordingly, wording along the following lines should be

inserted "which purports to identify". Yet another suggestion was that "person" should be replaced by the term "subject", which was a term of art widely used in practice and would appropriately cover the situation in which the subject of the certificate was not a person but a "device or electronic agent". That suggestion was opposed on the grounds that: if used, the term "subject" would need to be defined by reference to a "person"; a person would, in any case, control any "device or electronic agent"; and the term "subject" would be inconsistent with the terminology used in the Model Law, as well as in other UNCITRAL texts. While reference to a "person" was found to be acceptable, it was stated that it should be made clear that it meant the subject of a certificate and covered "entity" as well. As to the reference to "entity", it was agreed that it could be retained pending final determination by the Working Group of the question whether a "device or electronic agent" could be subject of a certificate. Yet another suggestion was that "a key pair" should be substituted for "a private key".

120. After discussion, the Working Group decided that the definition should be reformulated along the following lines:

"[Identity] certificate

"For the purposes of these rules, [identity] 'certificate' means a data message or other record which is issued by a certification authority and which purports to confirm the identity [or other significant characteristic] of a person or entity who holds a particular key pair".

121. It was agreed that the word "identity" and the words "other significant characteristic" that appeared within square brackets would allow the Working Group to consider at a later stage the question whether types of certificates other than identity certificates should be covered.

Provision on the minimum contents of an identity certificate

122. The Working Group next turned its attention to subparagraphs (a) through (e), focusing on the question whether they accurately described the minimum contents of an identity certificate.

General remarks

123. It was generally agreed that the practical purpose of a provision listing the minimum contents of a certificate was to set the standards that a certification authority would have to meet in order to fulfil its function and to avoid liability for damage caused as a result of the failure of the certification authority to include in the certificate all the necessary elements. It was widely felt that no final decision could be made with regard to the minimum contents of a certificate before the issue of liability of the certification authority and the question of the types of certificates to be covered had been clarified. The Working Group decided to proceed with its consideration of subparagraphs (a) to (e) on the assumption that a preliminary exchange of views might facilitate the resumption of the discussion at a later stage.

124. In the discussion, the question was raised whether a certificate that did not meet the minimum requirements set forth in draft article 8 should be considered as an invalid certificate or whether draft article 8 should function as a default rule with the result that such a certificate could be valid if agreed upon by the parties. In the latter case, it was suggested that a rule along the lines of draft article 5(2) should be inserted in draft article 8.

Chapeau

125. While it was agreed that a certificate could be issued in a purely paper form, the appropriateness of using the term "or other record" was questioned (see above, para. 118).

Subparagraph (a)

126. The substance of subparagraph (a) was found to be generally acceptable.

Subparagraph (b)

127. It was observed that use of the word "holder" raised the question whether the person to whom the certificate was issued or the person holding a copy of the certificate and relying thereon was meant. In addition, it was stated that use of the term "holder" created uncertainty since that term was used in draft article 8 to refer both to the person holding the certificate and to the person holding the relevant key pair. While it was suggested that use of the term "subject" should be preferred, for the reasons mentioned above, the Working Group expressed a general preference in favour of the term "person" (see above, para. 119). However, it was decided that both terms should be retained within square brackets for further consideration of the matter. As to the reference to a "device or electronic agent", the use of which was said to raise uncertainty, it was decided that they should be placed within square brackets pending further consideration of the matter by the Working Group (see above, para. 119).

Subparagraph (c)

128. The substance of subparagraph (c) was found to be generally acceptable. As to the word "holder", it was decided that it should be replaced by the words "subject" and "person" within square brackets (see above, para. 127).

Subparagraph (d)

129. It was generally agreed that the operational period was one of the most essential elements of a certificate. With regard to the reference to the scope of a certificate and any existing restriction thereon, it was suggested that it should be deleted or at least amended to specify that the scope and any restriction thereon could be incorporated in the certificate by reference. In support of that suggestion, it was stated that a complete listing of all restrictions might be impossible to include in a certificate. In addition, it was observed that such a reference could inadvertently result in the certification authority being liable for failing to include all possible restrictions in the certificate. That suggestion was opposed on the grounds that the scope and any restriction thereon were critical

elements on the basis of which the function and the integrity of a certificate could be assessed. In addition, it was stated that a reference to the scope of the certificate and any restriction thereon could address the need to indicate that certificates might fulfil various functions. It was thus suggested that such a reference should be included in a new subparagraph (f) within square brackets for further consideration of the matter by the Working Group. Subject to that change, the Working Group approved the substance of subparagraph (d).

Subparagraph (e)

130. While it was generally agreed that the signature of the certification authority was one of the essential elements of a certificate, differing views were expressed as to whether that signature needed to be digital. One view was that the signature should be digital in order to ensure integrity of the certificate. Another view was that, if the signature of the certification authority were cryptographic, relying parties might not be able to determine that it was the signature of a certain certification authority which would indicate its intent to be bound by the certificate. In addition, it was stated that, if the signature of the certification authority were not the result of a transparent procedure, the certificate might not be valid. The Working Group agreed that there was a need to ensure that the signature of the certification authority should be secure and the process should be transparent. Accordingly, it was decided that the word "digitally" should be retained without brackets and the words "or otherwise secured" should be added, in order to address the concerns expressed with regard to the term "digitally".

New subparagraph (g)

131. It was suggested that the algorithms applied by the certification authority should be listed as one of the minimum elements of a certificate. In support of that suggestion, it was stated that the algorithms were essential for ensuring identification of the signer and integrity of the data message. The suggestion was opposed on the ground that, if a reference to the relevant algorithms were required for the certificate to be valid, the certification authority could escape liability by not including them in the certificate. It was stated that, while it was necessary to ensure data integrity, that result might be better accomplished by including the element of data integrity in the definition of digital signature. A contrary view was the non-inclusion of the applied algorithms in the certificate would make the certification authority liable for failing to issue a valid certificate. After discussion, the Working Group decided to include a reference to the applied algorithms in draft article 8 within square brackets for further consideration of the matter at a future session.

Article 9. Certification practice statement

132. The text of draft article 9 as considered by the Working Group was as follows:

> "For the purposes of these Rules, "certification practice statement" means a statement published by a certification authority that specifies the practices that the certification authority employs in issuing and otherwise handling certificates."

133. The Working Group noted that draft article 9 related to a number of issues dealt with in other provisions of the Uniform Rules, e.g., the issue of representations upon issuance of a certificate (draft article 10) and the issue of liability of a certification authority (draft article 12) and decided to defer its consideration of draft article 9 until it had completed its consideration of the Uniform Rules.

Article 10. Representations upon issuance of certificate

134. The text of draft article 10 as considered by the Working Group was as follows:

"Variant A

"(1) By issuing a certificate, a certification authority represents to any person who reasonably relies on the certificate, or on a digital signature verifiable by the public key listed in the certificate, that:

"(a) the certification authority has complied with all applicable requirements of these Rules in issuing the certificate and, if the certification authority has published the certificate or otherwise made it available to such a relying person, that the holder listed in the certificate [and rightfully holding the corresponding private key] has accepted it;

"(b) the holder identified in the certificate [rightfully] holds the private key corresponding to the public key listed in the certificate;

"(c) the holder's public key and private key constitute a functioning key pair;

"(d) all information in the certificate is accurate as of the date it was issued, unless the certification authority has stated in the certificate [or incorporated by reference in the certificate a statement] that the accuracy of specified information is not confirmed; and

"(e) to the certification authority's knowledge, there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of the foregoing representations.

"(2) Subject to paragraph (1), the certification authority which issues a certificate represents to any person who reasonably relies on the certificate, or on a digital signature verifiable by the public key listed in the certificate, that the certification authority has issued the certificate in accordance with any applicable certification practice statement [incorporated by reference in the certificate, or] of which the relying person has notice.

Variant B

"(1) By issuing a certificate, a certification authority represents to the holder, and to any person who relies on information contained in the certificate[, in good faith and] during its operational period, that:

"(a) the certification authority has [processed] [approved] [issued], and will manage and revoke if necessary, the certificate in accordance with:

"(i) these Rules;

"(ii) any other applicable law governing the issuance of the certificate; and

"(iii) any applicable certification practice statement stated or incorporated by reference in the certificate, or of which such person has notice, if any;

"(b) the certification authority has verified the identity of the holder to the extent stated in the certificate or any applicable certification practice statement, or in the absence of such a certification practice statement, the certification authority has verified the identity of the holder in a [reliable] [trustworthy] manner;

"(c) the certification authority has verified that the person requesting the certificate holds the private key corresponding to the public key listed in the certificate;

"(d) except as set forth in the certificate or any applicable certification practice statement, to the certification authority's knowledge, all other information in the certificate is accurate as of the date the certificate was issued;

"(e) if the certification authority has published the certificate, the holder identified in the certificate has accepted it.

"[(2) If a certification authority issued the certificate subject to the laws of another jurisdiction, the certification authority also makes all warranties and representations, if any, otherwise applicable under the law governing its issuance.]"

135. It was suggested that the title of the draft article might read along the lines of "process of issuing a certificate". It was noted, at the outset, that draft article 10, which set a standard against which the liability of the certification authority was to be measured, was closely related to draft article 12, which provided the sanction to that standard. Based on Variant A, the discussion focused on whether the representations listed in subparagraphs (a) to (e) of paragraph (1) should be regarded as mandatory requirements (i.e., minimum standards from which the parties could not derogate by agreement) or as "default" rules. As to the meaning of possible "default rules", at various times in the discussion, "default" rules were characterized either as "gap-filling" rules (i.e., requirements that would only be binding in the absence of a contrary agreement) or as rules to be

applied only where no contract whatsoever existed between the parties.

136. In support of making paragraph (1) a default rule, it was stated that: a flexible rule was needed to ensure that the forthcoming changes in technology could be accommodated; imposing a high liability standard on all certification authorities would only result in hampering the development of the industry, while encouraging the less reliable certification authorities to enter the market; imposing minimum standards on relatively low-security certificates could restrict the global use of such certificates in a variety of important contexts; in general the expectations of the holder of the certificate and the relying parties with regard to the content of the certificate should only be determined by reference to what the certification authority had undertaken, in its certification practice statement or otherwise, to represent in the certificate; and adoption of mandatory minimum standards for certificates could leave the Uniform Rules isolated from actual commercial practice in major markets. Accordingly, the liability of the certification authority should only be determined by reference to obligations which the certification authority had accepted to undertake. Such an approach was said to provide the level of flexibility that was necessary to accommodate the wide variety of certificates that were available on the market. The following was suggested as a possible reformulation of draft article 10, which might be merged with draft article 12:

> "(1) A certification authority shall state explicitly in the certificate what kind of service it provides. If the obligation of the certification authority is not expressed in the certificate, the certification authority is deemed to have guaranteed the identity of the key holder.
>
> "(2) If a certification authority has failed to perform the services stated in the certificate or has guaranteed the identity of the key holder negligently, it is liable to the relying party for damages.
>
> "(3) A certification authority may limit its liability to pay damages by making explicit disclaimers in the certificate.
>
> "(4) This article is subject to contrary agreement between the certification authority and the relying party."

137. That proposal was objected to on the grounds that, in certain legal systems, there would be an inconsistency between defining the criteria under which a certificate might be accorded legal status on the one hand, and providing on the other hand that a general disclaimer could be used to disregard these essential criteria. It was also stated that there would typically exist no contractual relationship between the relying party and the certification authority. In that connection, the view was expressed that it might be useful to clarify whether the notion of "relying party" should encompass the holder of the key pair listed in the certificate. The view was also expressed that certificates might be very limited in size, thus making it difficult to include "explicit disclaimers" in the certificates. In response, it was stated that establishing a minimum standard as to the deemed contents of a certificate was in line with the need to reduce the size of the certificate itself.

138. In support of maintaining paragraph (1) of Variant A as a minimum standard from which the parties should not be allowed to derogate by private agreement, it was recalled that the Working Group at its previous session had expressly made a decision regarding that point (see A/CN.9/437, paras. 70-71). Moreover, it was stated that establishing minimum requirements, in addition to protecting the holder of the certificate and other relying parties, would also enhance the trustworthiness and the commercial acceptability of digital signature mechanisms, thus benefiting certification authorities as well. In response to an objection that establishing a minimum standard would result in imposing burdensome obligations on certification authorities, it was pointed out that the purpose of draft article 10 was not to impose any obligation on the certification authority but merely to define a specific legal regime for certain certificates which, by meeting certain requirements, would qualify to be granted a specific legal status. A certification authority would remain free to offer lower-quality certificates, although such certificates would not entail the same legal consequences. It was conceded by proponents of the retention of a minimum standard that mechanisms limiting the amount of liability under draft article 12 would appropriately balance the acceptance by certification authorities of mandatory requirements under draft article 10. A parallel was drawn in that respect with the liability regime in the maritime transport industry, where the interplay of unfettered market forces had historically resulted in general uncertainty of a magnitude such that it discouraged parties from entering into maritime transactions, thus creating a need for the earlier international instruments in that field, such as the Hague Rules.

139. It was suggested that limiting the scope of the provision by defining a specific type of certificate (e.g., identity certificates issued for the purposes of high-value transactions) to which draft article 10 would apply might make it more acceptable to formulate draft article 10 in terms of a mandatory standard. Alternatively, it was suggested that adopting a reduced mandatory standard might help to make acceptable the application of draft article 10 to a wider category of certificates. With a view to combining those two suggestions, a proposal was made that only subparagraphs (a), (d) and (e) of paragraph (1) should be retained as a minimum standard. While general support was expressed in favour of including that proposal in the continuation of the discussion, it was generally felt that further clarification would need to be provided on a number of issues.

140. One issue to be clarified was the exact category of certificates to which such a reduced mandatory standard would apply. One view was that the reduced standard should only apply to a limited category of high-security identity certificates. Support was expressed for the view that a stricter standard would be needed for those certificates to which a high level of legal certainty would attach. In particular, should the certificate be aimed at creating a legally-binding signature, further assurances would need to be provided as to the link between the certificate and the identity of the holder of the key pair. However, support was also expressed for the view that the proposed minimum standard under subparagraphs (a), (d) and (e) was so reduced that it could be made applicable to a broad range of certificates.

141. Another issue to be further clarified was the consistency of the proposed text of paragraph (1) with other provisions of the Uniform Rules dealing with the identification function of the certificate. It was recalled that, for the purposes of digital signatures, the main function of the certificate was to provide identification of the holder of the key pair, a reason why it had earlier been suggested that the Working Group should focus its attention on the notion of "identity"

certificates. Should the proposed reduced standard be adopted, the certification authority would no longer make any representation as to the identity of the holder but it would merely guarantee that the process defined by the certification authority itself had been followed. While it was recognized that such a process might indirectly lead to the identification of the holder of the key pair, it was suggested that further consideration might be given to retaining the substance of subparagraphs (b) and (c), dealing with the direct (or "conclusive") identification of the holder, in the Uniform Rules, possibly as part of draft article 2.

142. Although subparagraphs (a), (d) and (e) were suggested as setting a standard for identity certificates, it was generally agreed after discussion that such a limited standard could more appropriately apply to a wide variety of certificates. It was also agreed that further thought should be given to the manner in which the identification function should be reflected, either in draft article 10 or in an earlier part of the Uniform Rules, as an essential function of a smaller category of certificates, for which a high level of legal reliability was sought. It was agreed that the matter would need to be further discussed at a future session. Pending that discussion, subparagraphs (a), (d) and (c) would be maintained in paragraph (1) and subparagraphs (b) and (c) would be placed within square brackets. A suggestion was made that alternative wording drawn from paragraph (1)(b) of Variant B might need to be placed within square brackets in paragraph (1) for consideration by the Working Group at a future session. With respect to subparagraph (d), it was widely felt that the reference to a possible disclaimer by the certification authority as to the accuracy of the information contained in the certificate would be acceptable only if subparagraphs (b) and (c) were made part of paragraph (1).

143. With respect to paragraph (2), there was general agreement that the principle that a certification authority should abide by the commitments it had made in its certification practice statement should be retained.

144. Aimed at reflecting the above discussion, the following suggestion was made for a revised version of draft article 10:

"When a certificate is issued, it is deemed that:

(a) the person or entity issuing the certificate has complied with all applicable requirements of the Rules;

[(b) at the time of issuing the certificate, the private key is that of the holder and it corresponds to the public key listed in the certificate;]

[(c) the holder's public key and private key constitute a functioning key pair;]

(d) all information in the certificate is accurate as of the date it was issued[, unless the certification authority has stated in the certificate that the accuracy of specified information is not confirmed];

(e) to the certification authority's knowledge, there are no known, material facts

omitted from the certificate which would, if known, adversely affect the reliability of the information in the certificate; and

[(f) if the certification authority has published a certification practice statement, the certificate has been issued by the certification authority in accordance with that certification practice statement.]"

145. After discussion, the Working Group requested the Secretariat to prepare a revised draft of article 10, with possible variants, to reflect the above discussion.

Article 11. Contractual liability

146. The text of draft article 11 as considered by the Working Group was as follows:

"(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other party having a contractual relationship with the certification authority], the rights and obligations of the parties are determined by their agreement.

"(2) Subject to article 10, a certification authority may, by agreement, exempt itself from liability for any loss due to defects in the information listed in the certificate, technical breakdowns or similar circumstances. However, the clause which limits or excludes the liability of the certification authority may not be invoked if exclusion or limitation of contractual liability would be grossly unfair, having regard to the purpose of the contract.

"(3) The certification authority is not entitled to limit its liability if it is proved that the loss resulted from the act or omission of the certification authority done with intent to cause damage or recklessly and with knowledge that damage would probably result."

147. It was noted that paragraph (1) restated the principle of party autonomy in connection with the liability regime applicable to the certification authority. In addition, it was noted that paragraph (2) dealt with the issue of exemption clauses, which were generally declared admissible, with two exceptions. The first exception came from a reference to draft article 10, which was intended to set a minimum standard from which certification authorities should not be allowed to derogate. The second exception was inspired by the UNIDROIT Principles on International Commercial Contracts (Article 7.1.6), as an attempt to provide a uniform standard for assessing the general acceptability of exemption clauses. Moreover, it was noted that paragraph (3) dealt with the situation where loss or other damage would result from intentional misconduct by the certification authority or its agents (inspired by article 18 of the UNCITRAL Model Law on International Credit Transfers).

148. The Working Group considered first the question whether draft article 11 should be retained as part of the Uniform Rules. In support of deletion, it was stated that it dealt with matters that were better left to the contract and to the applicable law. In particular, it was observed that:

paragraph (1) was redundant, since it merely stated the principle of party autonomy, which was covered by article 4 of the Model Law; and paragraphs (2) and (3) were interfering with national law on matters which might not lend themselves to unification. In addition, it was observed that draft article 10 sufficiently covered the matter. While leaving the issues of contractual liability to the contract and to the law applicable outside the Uniform Rules was found to be an acceptable alternative, the prevailing view was that it was worth trying to achieve a degree of unification on this important matter.

149. As to the way in which that result could be achieved, a number of suggestions were made. One suggestion was to retain draft article 11 in its current formulation. In support of that suggestion, it was observed that, while paragraph (1) might appear as stating the obvious, paragraph (2) introduced the very important principle that the core obligations of the contract could not be taken away through exemption clauses. In addition, it was pointed out that paragraph (3) was essential and covered not only contractual but also non-contractual relationships.

150. Another suggestion was to refer in paragraph (1) to the inability of the parties to agree on "grossly unfair" terms and to delete paragraphs (2) and (3). While support was expressed for the deletion of paragraphs (2) and (3), that suggestion was objected to on several grounds, including that: use of the term "grossly unfair" was not appropriate, since it was unknown to many legal systems; the protection of the weaker party aimed at by this term should be left to other law (e.g. consumer protection law); and the deletion of paragraphs (2) and (3) could inadvertently result in allowing parties to nullify the core effect of the contract or to exempt liability for intentional misconduct.

151. A related suggestion was to insert after the word "obligations" in paragraph (1) the words "and any limitation thereon" and at the end the words "subject to applicable law", and to delete paragraphs (2) and (3). In support of that suggestion, it was said that such an approach would result in an acceptable general statement based on party autonomy and the applicable law. It was observed, however, that no unification would be achieved if that approach were to be adopted.

152. Yet another suggestion was to replace draft article 11 with a provision stating that the standards up to which the certification authority should be held liable should be those set forth in the certification practice statement. The suggestion was opposed on the ground that it would replace both the contract and the minimum standards set forth in draft article 10 as a point of reference for measuring the certification authority's liability. The view was expressed, however, that that suggestion might provide an appropriate rule for low security certificates to which the minimum standards of draft article 10 would not be applicable.

153. In the discussion, a number of suggestions of a drafting nature were made. With regard to paragraph (1), one suggestion was that the reference within square brackets to "any party" was too broad and vague and should be replaced by a reference to "any relying party". Another suggestion was that paragraph (1) should be amended to make it clear that it was not intended to subject the relationship between the parties exclusively to their agreement, since such an approach would make the exception to the right of the parties to agree on liability exemption clauses contained in paragraphs (2) and (3) meaningless. With regard to paragraph (2), it was suggested that after the

word "loss" the words "associated with the certificate" should be added and the remainder of the first sentence of paragraph (2) could be deleted.

154. After discussion, the Working Group failed to reach agreement as to the particular formulation of draft article 11 and requested the Secretariat to prepare alternative drafts reflecting the various views expressed for consideration at a future session.

Article 12. Liability of the certification authority to parties relying on certificates

155. The text of draft article 12 as considered by the Working Group was as follows:

"(1) In the absence of a contrary agreement, a certification authority which issues a certificate is liable to any person who reasonably relies on the certificate for:

"(a) [breach of warranty under article 10] [negligence in misrepresenting the correctness of the information stated in the certificate];

"(b) registering revocation of a certificate promptly upon receipt of notice of revocation of a certificate; and

"(c) [the consequences of not] [negligence in] following:

"(i) any procedure set forth in the certification practice statement published by the certification authority; or

"(ii) any procedure set forth in applicable law.

"(2) Notwithstanding paragraph (1), a certification authority is not liable if it can demonstrate that the certification authority or its agents have taken all necessary measures to avoid errors in the certificate or that it was impossible for the certification authority or its agents to take such measures.

"(3) Notwithstanding paragraph (1), a certification authority may, in the certificate [or otherwise], limit the purpose for which the certificate may be used. The certification authority shall not be held liable for damages arising from use of the certificate for any other purpose.

"(4) Notwithstanding paragraph (1), a certification authority may, in the certificate [or otherwise], limit the value of transactions for which the certificate is valid. The certification authority shall not be held liable for damages in excess of that value limit."

General remarks

156. Widespread support was expressed in favour of a provision dealing with the issue of liability of certification authorities towards relying parties along the lines of draft article 12. It was widely felt, however, that the scope of such a provision should be limited to cases in which the certification authority guaranteed the identity of the key holder and the integrity of the data messages signed by the key holder. Such an approach could facilitate certain practices in which high security standards were required, without negatively affecting other practices in which such high security and liability standards might not be appropriate.

157. Some doubt was expressed, however, as to whether a specific liability regime could or should be established. It was stated that introducing such a liability regime could hamper certification practices, if it were not accompanied by a reasonable quantification of the risks associated with the provision of certification services, since certification authorities would be exposed to risks for which they would not be able to obtain insurance coverage. In addition, it was observed that such a liability regime might not be necessary, since, in the absence of a specific regime, general principles of tort law would apply. It was pointed out, however, that in some jurisdictions in which the liability of certification authorities had not been regulated specifically, certification authorities would, in principle, not be liable towards relying parties. In addition, it was said that leaving the matter to the applicable law would not be appropriate for a number of reasons, including that: the uncertainty prevailing in many jurisdictions could negatively affect the development of electronic commerce; the absence of any liability could inadvertently result in business parties being unable to take advantage of the services offered by certification authorities; and the determination of the applicable law raised very difficult questions. As to the form of the work product, the view was expressed that a uniform liability regime could be implemented more effectively by way of a convention than through a model law (see below, para.212).

158. After discussion, the Working Group decided that every effort should be made to address the issue of liability of certification authorities towards relying parties in the Uniform Rules and went on to consider draft article 12 in detail. It was suggested that the Working Group might wish to include in the future discussion of draft article 12 a consideration of the nature and foreseeability of damages incurred by the relying party.

Paragraph (1)

Chapeau

159. Differing views were expressed as to whether the opening words of the chapeau should be retained. One view was that, if draft article 10 set minimum standards that the certification authority had to meet, the opening words should be deleted. Another view was that the opening words were useful and should be retained, to the extent that they allowed parties to negotiate their liability. It was stated in response that parties could not negotiate, since draft article 12 dealt with tortious liability in cases in which, typically, there was no agreement. It was observed, however, that relying parties in closed communication systems would normally have some type of agreement with the certification authority. In addition, it was observed that liability terms negotiated between

certification authorities and key holders might be incorporated in contracts between key holders and relying parties.

160. The prevailing view was that the cases mentioned were exceptional and should not be allowed to defeat the main purpose of draft article 12 which was to regulate tortious liability of certification authorities towards third parties. It was thus suggested that the residual need to address contrary agreements between certification authorities and their clients or relying parties, whenever such agreements existed, could be addressed by including appropriate wording at the end of draft article 12.

Subparagraphs (a) to (c)

161. It was observed that the second set of bracketed language in subparagraphs (a) and (c) appeared to reflect the principle of strict liability and should be deleted. The concern was expressed that use of the notion of "misrepresentation" might create uncertainty, since it had a specific meaning in some legal systems but was unknown in other legal systems. "Mis-statements" was suggested as an alternative expression.

Paragraph (2)

162. Differing views were expressed as to whether the burden of proof of negligence should be on the certification authority or on the relying party. One view was that the burden of proof should be on the relying party. In support, it was stated that the relying party could prove negligence, since the evidence as to whether the certification authority had met the standard of care set forth in draft article 10 would be readily available to the relying party. In addition, it was pointed out that shifting the burden of proof to the certification authority would be appropriate only if the Working Group had adopted the principle of strict liability. Another view was that, while liability should be based on negligence, the burden of proof should be placed on the certification authority, since any relevant evidence would be under the control of the certification authority. It was observed that that would be the case, in particular, if the certificate referred not to the identity of the key holder but to the procedure followed by the certification authority to determine the identity of the key holder.

Paragraphs (3) and (4)

163. Support was expressed in favour of the principle of limitation of the liability of the certification authority embodied in paragraphs (3) and (4). However, the view was expressed that limits of liability would be appropriate only in case of a regime based on strict liability of the certification authority, as opposed to a liability regime based on negligence.

164. As to the types of limits that could be introduced, it was stated that a monetary limit per transaction did not adequately protect certification authorities, particularly in the context of identity certificates, since, irrespective of the liability limit, they could be used several times within a very short period of time, without there being a way to determine whether the liability limit had been exceeded. It was, therefore, suggested that a provision introducing an aggregate liability limit

should be included in draft article 12 that could read along the following lines: "A certification authority may, in the certificate or otherwise, provide a limit of liability for the lifetime of the certificate for all incidents of reliance in the amount of an aggregate value of the certificate. The certification authority shall not be held liable for damages in excess of that aggregate limit regardless of the number of claims made against that certificate". The view was expressed, however, that aggregate liability limits could not function since a relying party would have no way of knowing, under existing technology applications, whether a certain limit had been reached.

Proposals for new draft article 12

165. In order to address the concerns expressed above, a number of proposals for an alternative formulation of draft article 12 were made. One proposal was that draft article 12 should read along the following lines:

"(1) Where a certification authority issues a certificate, it is liable to any person who reasonably relies on the certificate, if it is negligent by:

"(a) providing incorrect information in the certificate;

"(b) failing to [notify or] publish the revocation [or suspension] of the certificate promptly upon becoming aware of the need to revoke [or suspend] it[; or

"(c) failing to follow a procedure in a certification practice statement which has been published by the certification authority and of which the relying person has had notice].

"(2) A certification authority may state in the certificate [or elsewhere] a restriction on the purpose or purposes for which the certificate may be used and the certification authority shall not be liable for damage arising from use of the certificate for any other purpose.

"(3) A certification authority may state in the certificate [or elsewhere] a limit on the value of transactions for which the certificate is valid and the certification authority shall not be liable for damages in excess of that limit.

"[(4) Paragraph (1) of this article does not apply if, and to the extent that, there are contrary terms in an agreement between the certification authority and the person who relies on the certificate.]"

166. Another proposal was that draft article 12 should be amended to read as follows:

"(1) Unless a certification authority proves that it or its agents have taken all reasonable measures to avoid errors in the certificate, it is liable to any person who reasonably relies on a certificate issued by that certification authority for:

"[insert subparagraphs (a) to (c)]

"(2) Notwithstanding paragraph (1), reliance on a certificate is not reasonable to the extent that it is contrary to the information contained in the certificate."

167. While the first proposal was met with some interest, the Working Group focused its discussion on the second proposal. It was stated that paragraph (1) was intended to establish liability for errors in the certificate subject to the principle of reasonable reliance, avoiding any reference to representations and negligence. In addition, it was observed that paragraph (2) was aimed at allowing the certification authority to set forth in the certificate the standards against which the reasonableness of the reliance on the certificate would be tested. It was explained that paragraph (2) was not intended to provide an exhaustive list of all situations in which reliance on the certificate would not be reasonable. While paragraphs (1) and (2) were generally felt to be acceptable as a basis for future discussion, a number of concerns were expressed and suggestions made.

New paragraph (1)

168. One concern was that, in practice, it would be almost impossible for certification authorities to take "all reasonable measures" in a cost- and time-effective manner. In order to address that concern, a number of suggestions were made. One suggestion was that the word "commercially" should be substituted for the word "all". In support of that suggestion, it was stated that a reference to "commercially reasonable measures" would reflect what was practicable under the particular circumstances. In addition, it was observed that such a reference would be in line with terminology used in other UNCITRAL texts (e.g., article 5(2)(a) of the UNCITRAL Model Law on International Credit Transfers). The suggestion was opposed on the ground that it would introduce uncertainty, in view of the fact that there existed no universal understanding of what was "commercially reasonable". Another suggestion was that the term "all" should be simply deleted. That suggestion too was opposed on the ground that it might inadvertently result in inappropriately lowering the standard of care to be met by certification authorities. Yet another suggestion was that language used in article 7(1)(b) of the Model Law should be used in new paragraph (1).

169. Another concern was that new paragraph (1) failed to address errors made by the certification authority in issuing a certificate. In order to address that concern, it was suggested that the words "or issuing it" be added after "certificate" in new paragraph (1). It was stated that information contained in a certificate revocation list (CRL) or similar list should also be covered in new paragraph (2).

170. It was agreed that, pending determination of the question of the function of certification practice statements, subparagraph (c) should be placed within square brackets.

New paragraph (2)

171. As a matter of drafting, it was suggested that the opening words should be deleted and the words "subject to paragraph (2)" should be inserted at the beginning of new paragraph (1). The concern was expressed that new paragraph (2) could have the unintended result of excessively limiting the grounds on which the reasonableness of the reliance on the certificate could be

questioned. Another concern was that new paragraph (2) might not cover a situation in which the certificate might be relied upon in a transaction of an excessive value, since value might not be covered by the term "information". In order to address those concerns, it was suggested that paragraphs (3) and (4) of draft article 12 should be listed as examples of situations in which reliance on the certificate would not be reasonable. In the same vein, it was suggested that other similar examples might be given relating, e.g., to situations in which the certification authority might state in the certificate which designated parties or types of parties might rely on that certificate. In addition, it was suggested that the certification authority should not be able to rely on limits of liability if the loss resulted from intentional or reckless behaviour of the certification authority.

172. Another concern was that, by referring to the information "contained" in the certificate, new paragraph (2) might inadvertently result in inappropriately increasing the amount of information that would need to be included in a certificate. In order to address that concern, the suggestion was made that incorporation of that information in the certificate by reference should be allowed. That suggestion was opposed on the ground that it would be unfair to subject the rights of third parties to terms incorporated in an agreement between the certification authority and the key holder, since those terms might not even be readily available to third parties.

173. After discussion, the Working Group decided that draft article 12 should be reformulated along the following lines:

> "(1) Subject to paragraph (2), unless a certification authority proves that it or its agents have taken [all reasonable] [commercially reasonable] measures [that were appropriate for the purpose for which the certificate was issued, in the light of all circumstances] to avoid errors in the certificate [or in issuing it], it is liable to any person who reasonably relies on a certificate issued by that certification authority for:
>
> > "(a) errors in the certificate; [or]
> >
> > "(b) registering revocation of a certificate promptly upon receipt of notice of revocation of a certificate[; or
> >
> > "(c) the consequences of not following:
> >
> > > "(i) any procedure set forth in the certification practice statement published by the certification authority; or
> > >
> > > "(ii) any procedure set forth in applicable law].
>
> "(2) Reliance on a certificate is not reasonable to the extent that it is contrary to the information contained [or incorporated by reference] in the certificate [or in a revocation list] [or in the revocation information]. [Reliance is not reasonable, in particular, if:
>
> > "(a) it is contrary to the purpose for which the certificate was issued;

"(b) it exceeds the value for which the certificate is valid; or

"(c) [...]."

The view was expressed that draft article 12 should apply only to certification authorities issuing identity certificates.

Articles 13 to 16

174. For lack of sufficient time, the Working Group postponed its consideration of draft articles 13 to 16 to a future session. The view was expressed that these draft articles should apply only to certification authorities issuing identity certificates. Another view was that the Working Group should consider whether the Uniform Rules should apply only to identity certificates or to any other kind of certificate.

CHAPTER IV. RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES

Article 17. Foreign certification authorities offering services under these Rules

175. The text of draft article 17 as considered by the Working Group was as follows:

"Variant A (1) Foreign [persons] [entities] may become locally established as certification authorities or may provide certification services from another country without a local establishment if they meet the same objective standards and follow the same procedures as domestic entities and persons that may become certification authorities.

(2) "Variant X The rule stated in paragraph (1) does not apply to the following: [...].

"Variant Y Exceptions to the rule stated in paragraph (1) may be made to the extent required by national security.

"Variant B The ... *[the enacting State specifies the organ or authority competent to establish rules in connection with the approval of foreign certificates]* is authorized to approve foreign certificates and to lay down specific rules for such approval."

General remarks

176. With regard to the title of chapter IV, it was said that the reference therein to recognition of foreign electronic signatures was not appropriate, since the chapter dealt with the provision of

services by foreign certification authorities (i.e. draft article 17), the endorsement of foreign certificates by domestic certification authorities (i.e. draft article 18) and the recognition of foreign certificates (i.e. draft article 19). The Working Group considered briefly a number of suggestions that were made so as to reflect more clearly in the chapter heading the subject matter dealt with therein (e.g. "cross-border recognition of certificates", "recognition of electronic signatures and certificates", "recognition of foreign certification authorities and certificates"). However, it was generally agreed that the consideration of an appropriate heading for chapter IV should be postponed until the Working Group had discussed in more detail the legal effects of certificates.

177. With regard to the two variants proposed in draft article 17, it was generally felt that Variant B, which left for a specified organ of the enacting State to lay down rules for the approval of foreign certificates, did not provide an appropriate basis for the development of uniform rules. It was agreed that Variant B should be deleted and that the Working Group should focus its deliberations on Variant A.

Scope of draft article 17

178. It was pointed out that the objectives of draft article 17 were twofold: firstly, it recognized the right of a foreign certification authority to become locally established, under the conditions set forth therein; and secondly, it gave the foreign certification authorities the right to provide services in the enacting State without having a local establishment. As such, draft article 17 touched upon matters of trade policy, namely the extent to which the enacting State would waive restrictions against the establishment of foreign certification authorities and the provision of services by foreign certification authorities. It was suggested, instead, that the Working Group should attempt to focus its work on the development of model provisions on the legal effects of foreign certificates and the relationship between certificate holders and certification authorities. Various interventions were made in support of that view. It was felt that matters of trade policy fell within the province of other forums, and that it would not be advisable to address them in the Uniform Rules.

179. In response to those views it was noted that, by allowing foreign entities to become established as certification authorities, draft article 17 merely stated the principle that foreign entities should not be discriminated against, provided that they met the standards set forth for domestic certification authorities. That principle was found to be of particular relevance with respect to certification authorities, since they might be expected to operate without necessarily having a physical establishment or other place of business in the country in which they operated. It was further stated that the Model Law itself dealt with a number of cross-border matters which might be seen as raising issues of trade policy.

180. Having heard the various views expressed, and for the purpose of advancing its consideration of the Uniform Rules, the Working Group proceeded to discuss a number of amendments to draft article 17, without prejudice to the reservations that had been expressed in connection with the substance of draft article 17.

Paragraph (1)

181. The question was asked whether paragraph (1) contemplated only the recognition of certification authorities that operated pursuant to an approval issued by an organ or governmental agency of the foreign State. In response to that question it was observed that, as currently drafted, paragraph (1) did not touch upon the question of whether a certification authority required a governmental approval in the foreign State. However, the view was also expressed that a provision such as draft article 17 had to be based on a licensing regime pursuant to legislative requirements.

182. The view was expressed that some of the difficulties that had been raised by paragraph (1) stemmed from the fact that the provision seemed to place excessive emphasis on the recognition of the certification authority itself, rather than on the certification authority's ability to issue certificates that would be used in the enacting State. Furthermore, the phrase "meet the same objective standards and follow the same procedures as domestic entities and persons that may become certification authorities", might pose an obstacle to the use of new technologies, since the provision could be interpreted as providing grounds for barring the recognition of foreign certification authorities that followed procedures that were technologically more advanced than those in use in the enacting State. Instead of the current formulation, it was suggested that it would be preferable to make reference to "objective requirements" that had to be met by certification authorities in the enacting State. Alternatively, the words "and follow the same procedures" should be placed within square brackets.

183. In connection with the conditions to be met by a foreign certification authority, it was observed that the purpose of draft paragraph (1) was to ensure that those conditions would be essentially the same as those applying to national certification authorities. It was therefore proposed to redraft paragraph (1) to the effect that the recognition of foreign certification authorities should be subject to the laws of the enacting State. Questions relating to the definition of the standards that had to be met by the foreign certification authority could be considered by the Working Group at a later stage. In addition, such an amendment would make it clear that the recognition was also subject to any exclusions obtaining in the enacting State, thus obviating the need for either of the variants of paragraph (2). The proposed text was as follows:

"Subject to the laws of the enacting State, a foreign [person][entity] may:

"(a) become locally established as a certification authority; or

"(b) provide certification services without being established locally if it meets the same objective standards and follows the same procedures as domestic entities and persons that may become certification authorities."

184. In response to that proposal it was stated that the reference to domestic law was not a satisfactory solution since the laws of the enacting State might contain discriminatory provisions that might undermine the spirit of draft article 17. Furthermore, the proposed amendment gave rise to questions as to who in the enacting State would make a determination that the foreign

certification authority met the same objective standards and followed the same procedures as domestic entities and persons and by what means such a determination would be made.

185. The view was expressed that, in its present formulation, paragraph (1) seemed to imply that foreign certification authorities needed not only to be approved under their own law, but needed to comply in addition with the requirements of the enacting State. It was considered that such a rule might have undesirable restrictive effects and would not contribute to promoting electronic commerce. In connection with the latter observation it was suggested that the meaning of paragraph (1) might be clarified by recasting it as a non-discrimination rule along the following lines:

> "(1) Foreign [persons] [entities] may not be denied the right to become locally established or to provide certification services solely on the grounds that they are foreign if they meet the same objective standards and follow the same procedures as domestic entities and persons that may become certification authorities."

186. That proposal was objected to on the ground that the proposed rule of non-discrimination raised the same type of general concerns that had been raised in the general remarks concerning the scope of draft article 17 (see above, paras. 178-180).

187. Having considered the various proposals, and taking into account the differing views that had been expressed, the Working Group felt that more time for consultations was needed on the matters dealt with in paragraph (1). The Secretariat was requested to propose a revised version of paragraph (1), with possible variants reflecting the above discussion, for consideration by the Working Group at a later stage.

Paragraph (2)

188. In connection with the two variants of exclusions offered under paragraph (2), the view was expressed that Variant X should be deleted since it might provide an open-ended mechanism for limiting the scope of paragraph (1). Pursuant to that view, if any exclusion was to be allowed, it should only be on grounds of national security, as provided under Variant Y. However, general preference was expressed for retaining Variant X, pursuant to which it would be for the enacting State to formulate the exceptions to the general rule of paragraph (1). While Variant Y had the merit of limiting the possible exclusions to those that related to national security, it was felt that States might wish to include in their legislation other possible grounds for exclusions based on public policy. After discussion, it was decided that both Variants X and Y should be retained in square brackets for future consideration.

Article 18. Endorsement of foreign certificates by domestic certification authorities

189. The text of draft article 18 as considered by the Working Group was as follows:

> "Certificates issued by foreign certification authorities may be used for digital

signatures on the same terms as certificates subject to these Rules if they are recognized by a certification authority operating under ... *[the law of the enacting State]*, and that certification authority guarantees, to the same extent as its own certificates, the correctness of the details of the certificate as well as the certificate being valid and in force."

190. As a general remark, it was stated that the inclusion of provisions dealing with issues of cross-border recognition represented a significant step towards enhancing the trustworthiness of certificates. It was said that commercial practice was increasingly making use of certificates and that confidence in this new technology might be fostered through adherence to international standards. The Working Group was invited to consider international mechanisms for the accreditation of certification authorities that operated pursuant to international standards. Support was expressed to including the proposed topic among the matters to be discussed by the Working Group at a later stage. It was noted, however, that the proposed topic did not relate only to the matters raised in draft article 18 and that it might, for instance, be taken up by the Working Group when it resumed consideration of the issue of registration of certificates.

191. With regard to draft article 18, it was noted that the purpose of the rule contained therein was merely to enable a domestic certification authority to guarantee, to the same extent as its own certificates, the correctness of the details of the foreign certificate, and to guarantee that the foreign certificate was valid and in force. By virtue of draft article 18, the liability in the event that the foreign certificate was found to be defective was allocated to the domestic certification authority that provided such a guarantee. However, the existence of a guarantee pursuant to draft article 18 was not a necessary condition for the recognition of a certificate issued by foreign certification authorities that otherwise met the conditions set forth in draft article 19. To the extent that the provision of a guarantee under draft article 18 was merely voluntary, it was suggested that draft article 18 was not necessary and might be deleted. It was further suggested that the Uniform Rules should leave it for the enacting State to decide whether and under what conditions domestic certification authorities could provide such a guarantee in connection with certificates issued by foreign certification authorities. Reference to the issuance of guarantees of the type contemplated in draft article 18 might be made in a guide to enactment or in accompanying explanatory notes, depending on the nature of the instrument that was ultimately adopted.

192. The Working Group was reminded of its earlier discussions, during its thirty-first session, of the different levels of trustworthiness that could be provided by a domestic certification authority with respect to a foreign one. It was noted that those levels ranged from the highest level, in which the domestic certification authority, upon request of the party relying on a foreign certificate, guaranteed the contents of that certificate on the basis of its declared knowledge of the procedures that had led to the issuance of the certificate, thus assuming full liability for any errors or other defects in the certificate, to the lowest level of trustworthiness, where the domestic certification authority would merely guarantee the identity of the foreign certification authority, based on a verification of its public key and digital signature (see A/CN.9/437, paras. 81-82). It was suggested that those different levels of trustworthiness were not adequately reflected in draft article 18 and that, if the provision was retained, it should be made clear that it did not exclude arrangements other than a full guarantee of the correctness and validity of a certificate issued by a foreign certification authority.

193. In response to those observations it was stated that draft article 18 served a useful purpose, since it allowed the circulation and cross-border use of certificates without calling for bilateral or multilateral international agreements on the recognition of certificates which some States might consider to be required in order to grant recognition under draft article 19. Furthermore, in view of the decision made by the Working Group to deal in the Uniform Rules not only with certification authorities licensed by public entities but also with certification authorities that operated outside a governmental licensing scheme (see A/CN.9/437, paras. 48-50), draft article 18 had the additional advantage of allowing a commercial solution for situations in which recognition under draft article 19 would not be available automatically. In that connection, it was suggested that the scope of draft article 18 could be clarified by redrafting along the following lines:

> "Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as certificates subject to these Rules on the basis of an appropriate guarantee provided by a certification authority operating under ... *[the law of the enacting State]*."

194. Support was expressed in favour of retaining in the Uniform Rules a provision that authorized a domestic certification authority to provide guarantees in connection with certificates issued by foreign certification authorities. Such a provision might be based on draft article 18, taking into account the proposals made in the Working Group. However, it was suggested that the current location of draft article 18 in chapter IV was inadequate, since the provision did not deal with recognition of certificates issued abroad.

195. After deliberation, the Working Group agreed to retain draft article 18 within square brackets, with the proposed amendments, and requested the Secretariat to prepare alternative versions of that provision, taking into account the views that had been expressed, for future consideration by the Working Group.

Article 19. Recognition of foreign certificates

196. The text of draft article 19 as considered by the Working Group was as follows:

> "(1) Certificates issued by a foreign certification authority are recognized as legally equivalent to certificates issued by certification authorities operating under ... *[the law of the enacting State]* if the practices of the foreign certification authority provide a level of reliability at least equivalent to that required of certification authorities under these Rules. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]
>
> "(2) Signatures and records complying with the laws of another State relating to digital or other electronic signatures are recognized as legally equivalent to signatures and records complying with these Rules if the laws of the other State require a level of reliability at least equivalent to that required for such records and

signatures under ... *[the Law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

"(3) Digital signatures that are verified by reference to a certificate issued by a foreign certification authority shall be given effect [by courts and other finders of fact] if the certificate is as reliable as is appropriate for the purpose for which the certificate was issued, in light of all the circumstances.

"(4) Notwithstanding the preceding paragraph, Government agencies may specify [by publication] that a particular certification authority, class of certification authorities or class of certificates must be used in connection with messages or signatures submitted to those agencies."

Paragraphs (1) and (2)

197. It was observed that paragraphs (1) and (2) dealt with the ways in which the reliability of foreign certificates and signatures might be established in advance of any transaction being made (and any dispute arising as to the level of reliability of a signature). For that purpose, paragraphs (1) and (2) set forth the tests that might be applied in the enacting State in order to recognize the certificates issued by foreign certification authorities, as well as signatures and records complying with the laws of another State.

198. Various questions were raised concerning the scope of the recognition under paragraphs (1) and (2). With regard to paragraph (1), the view was expressed that the notion of legal equivalence between certificates issued by foreign certification authorities and certificates issued by certification authorities operating under the rules of the enacting State was not sufficiently clear. It was pointed out that the term "recognition", as commonly used in private international law, entailed the granting of legal effects to acts performed in another jurisdiction. However, that notion could not be applied in the context of paragraph (1), since a certificate was an instrument that contained statements of fact which merely fulfilled a declaratory function. Furthermore, both paragraph (1) and paragraph (2) implied that the enacting State should apply its own laws to ascertain the reliability of certificates issued by foreign certification authorities as well as signatures and records complying with the laws of another State. Therefore, it was said that paragraphs (1) and (2) were not in line with general principles of private international law pursuant to which the validity of acts performed abroad was to be settled in accordance with the applicable law of the jurisdiction where they had been accomplished. In addition, it was pointed out that article 13 of the Model Law and draft articles 3 and 5 of the Uniform Rules already provided rules for the attribution of data messages and for ascertaining the reliability of an electronic signature.

199. In response to those observations, it was pointed out that paragraphs (1) and (2) served a useful purpose in connection with national regulatory regimes that required the use of specified classes of certificates providing a high level of reliability for the performance of certain transactions. In enacting States that had such regulatory regimes, paragraph (1) provided

minimum standards for the recognition of certificates issued by foreign certification authorities that were used in connection with transactions other than those for which a specified class of certificates was required. By the same token, paragraph (2) provided those enacting States with a default rule that created a presumption of validity for signatures and records complying with the laws of another State which were found to provide a reasonable level of security for all those situations where no higher requirements were imposed under the laws of the enacting State. The Working Group was urged not to leave the issue of the minimum standards that applied to a foreign certificate to be settled entirely pursuant to the conflict-of-laws rules of the enacting State.

200. The Working Group discussed possible amendments to paragraphs (1) and (2) with a view to addressing the concerns that had been voiced. In particular, it was suggested that paragraphs (1) and (2) could be combined and reformulated as a non-discrimination rule along the following lines:

> "Certificates issued by foreign certification authorities shall not be precluded from having the same recognition as certificates issued by domestic certification authorities on the ground that they have been issued by foreign certification authorities."

201. However, objections were raised to the proposed negative formulation, since it did not provide the standards on the basis of which the recognition should be granted. Furthermore, it was observed that the proposed non-discrimination rule might give rise to the same reservations that had been voiced in connection with draft article 17 (see above, paras. 185-186).

202. After deliberation, it was generally felt that it would be desirable to formulate a substantive rule that provided a method for establishing the reliability of foreign certificates and signatures in advance of any transaction being made. The Secretariat was requested to prepare a revised version of paragraphs (1) and (2), including one that combined the two paragraphs, with possible variants taking into account the views that had been expressed.

Paragraph (3)

203. It was observed that paragraph (3) was intended to establish the standard against which foreign signatures and certificates might be assessed in the absence of any prior determination of their reliability. However, it was suggested that, as currently formulated, the provision might not be needed, since it merely restated the principle that, in the event that a dispute arose concerning the authenticity of a signature and the reliability of a certificate issued by a foreign certification authority, the courts of the enacting State had to give to such signature or certificate the evidentiary weight that was found to be appropriate in the circumstances.

204. In response to those observations it was noted that paragraph (3), which was inspired by article 7 of the Model Law, provided useful guidance for the courts of the enacting State in assessing the reliability of a foreign certificate. It was desirable to restate that important principle in the Uniform Rules in view of the fact that a State adopting the Uniform Rules might not necessarily have incorporated article 7 of the Model law in its domestic legislation. In order to state more clearly its purpose, it was proposed that paragraph (3) might be redrafted along the

following lines:

> "Digital signatures that are verified by reference to a certificate issued by a foreign certification authority shall not be precluded from being given effect [by courts and other finders of fact] if the certificate is as reliable as is appropriate for the purpose for which the certificate was issued, in light of all the circumstances."

205. After deliberation, the Working Group decided that the substance of paragraph (3) should be retained for further consideration by the Working Group at a later stage.

Paragraph (4)

206. Questions were raised concerning the need for a provision such as paragraph (4), which preserved the right of Government agencies to determine the procedures to be used in communicating electronically with them. On the one hand, the concern was expressed that paragraph (4) might have undesirable restrictive implications and might be interpreted to the effect that persons or entities other than Government agencies did not have the right to choose the particular certification authority, class of certification authorities or class of certificates that they wished to use in connection with messages or signatures they received. Such a situation was considered to be inconsistent with the principle of party autonomy enshrined in various provisions of the Model Law. On the other hand, if the purpose of paragraph (4) was to establish a special prerogative for Government agencies, the provision might need further refinement, since it might be construed to the effect that, in the absence of a clear indication by a Government agency of the particular certification authority, class of certification authorities or class of certificates that they wished to use in connection with messages or signatures submitted to them, the Government agency was under an obligation to accept any class of certification authority or certificate.

207. It was generally felt that parties to commercial and other transactions, and not only Government agencies, should be accorded the right to choose the particular certification authority, class of certification authorities or class of certificates that they wished to use in connection with messages or signatures they received. The Working Group requested the Secretariat to reformulate paragraph (4) so as to reflect that understanding and decided to consider the appropriate location for the revised provision at a later stage.

IV. COORDINATION OF WORK

208. The Working Group heard statements regarding work undertaken by the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the United Nations Conference on Trade and Development (UNCTAD) in the field of electronic commerce.

209. It was stated that, at its 29th general conference, UNESCO had received the mandate to undertake the preparation of an international legal instrument relating to the use of cyberspace. In that connection, the view was expressed that there was a need for UNESCO and UNCITRAL to

join their efforts in the field of electronic commerce. It was observed that those efforts should be guided by the need to promote electronic commerce in a manner that would benefit both developed and developing countries and that would, at the same time, guarantee the fundamental human rights, including the right to privacy. It was emphasized that issues of attribution of data messages to their originator, integrity of data messages and accountability of parties involved in electronic commerce should be at the core of the efforts of the Working Group on digital and other electronic signatures.

210. In a statement regarding the work of UNCTAD, it was observed that a Global Trade Point Network had been established, with the aim of assisting developing countries in their efforts to benefit from developments in the field of electronic communications. In addition, it was announced that UNCTAD was organizing an exhibition of manufacturers of equipment, producers of software and providers of services in electronic commerce (Lyon, 8-13 November 1998). The exhibition, it was observed, would include a series of presentations on a wide range of issues relating to electronic commerce.

211. The Working Group took note of the statements and welcomed the participation of interested organizations in its work. The Secretariat was requested to continue monitoring developments with respect to the legal issues of electronic commerce, as dealt with by other international organizations, and to report to the Working Group on those developments.

V. FUTURE WORK

212. At the close of the session, the proposal was made that the Working Group might wish to give preliminary consideration to undertaking the preparation of an international convention based on provisions of the Model Law and of the Uniform Rules. It was agreed that the topic might need to be taken up as an agenda item at the next session of the Working Group on the basis of more detailed proposals possibly to be made by interested delegations. However, the preliminary conclusion of the Working Group was that the preparation of a convention should in any event be regarded as a project separate from both the preparation of the Uniform Rules and any other possible addition to the Model Law. Pending a final decision as to the form of the Uniform Rules, the suggestion to prepare a convention at a later stage should not distract the Working Group from its current task, which was to focus on the preparation of draft uniform rules on digital and other electronic signatures, and from its current working assumption that the Uniform Rules would be in the form of draft legislative provisions. It was generally understood that the possible preparation of a draft convention should not be used as a means of reopening the issues settled in the Model Law, which might negatively affect the increased use of that already successful instrument.

213. It was noted that the next session of the Working Group was scheduled to be held in New York from 29 June to 10 July 1998, those dates being subject to confirmation by the Commission at its thirty-first session (New York, 1-12 June 1998).

Notes

1/ Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 223-224.

2/ Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.